NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE ENHANCED DRIVER'S LICENSE: COLLATERAL GAINS OR COLLATERAL DAMAGE?

by

James M. Clark

December 2012

Thesis Advisor: Carolyn Halladay
Second Reader: Erik Dahl

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2012	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE THE ENHANCED DRIVER'S LICENSE: COLLATERAL GAINS OR COLLATERAL DAMAGE?	5. FUNDING NUMBERS
6. AUTHOR(S) James M. Clark	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE A

13. ABSTRACT (maximum 200 words)

On a day-to-day basis, "security" to most Americans means proving their identity by producing a valid government-issued identification document (ID)—most commonly a driver's license. For this reason, terrorists on September 11, 2001, (9/11) placed high value on driver's licenses as a mean to mask preparatory activities leading up to their attack. Congress, as a result, enacted several measures, culminating in the Western Hemisphere Travel Initiative (WHTI), adopted June 1, 2009. The WHTI requires all citizens to show proof of identity while crossing U.S. land, sea, and recently some air borders between Canada, Mexico, the Caribbean, and Bermuda. To facilitate the initiative, the Department of Homeland Security (DHS) expanded on such ongoing ID initiatives as NEXUS, FAST, and SENTRI and adopted a number of different ID solutions, including passport card (PASS Card), Enhanced Driver's License (EDL), Global Entry and the Enhanced Tribal Card while considering others beyond the costly passport to facilitate commerce, trade, and tourism with Border States. All WHTI IDs employ vicinity-read radio frequency identification (RFID) technology, which has raised privacy concerns. This thesis seeks to join the ongoing civil liberties vs. national security debate through a case study of the EDL on both technological and legal grounds.

14. SUBJECT TERMS Department of Homeland Security, Western Hemisphere Travel Initiative, Customs Border Control, Enhanced Driver's License, Passport Card, NEXUS, FAST, SENTRI, Global Entry, Driver's License, REAL ID Act of 2005, Identification Documents, Vicinity Read, Proximity Read, Radio Frequency Identification, RFID, Barcode, Magnetic Stripe, Smart Card, Right to Privacy	15. NUMBER OF PAGES 113
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE ENHANCED DRIVER'S LICENSE: COLLATERAL GAINS OR COLLATERAL DAMAGE?

James M. Clark
Major, United States Air Force
A.S., Community College of Air Force, 1997
B.S., Troy State University, 2000
M.S., The University of Oklahoma, 2004
P.h.D., Capella University, 2007

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2012**

Author: James M. Clark

Approved by: Carolyn Halladay
Thesis Advisor

Erik Dahl
Second Reader

Harold Trinkunas
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

On a day-to-day basis, “security” to most Americans means proving their identity by producing a valid government-issued identification document (ID)—most commonly a driver’s license. For this reason, terrorists on September 11, 2001, (9/11) placed high value on driver’s licenses as a mean to mask preparatory activities leading up to their attack. Congress, as a result, enacted several measures, culminating in the Western Hemisphere Travel Initiative (WHTI), adopted June 1, 2009. The WHTI requires all citizens to show proof of identity while crossing U.S. land, sea, and recently some air borders between Canada, Mexico, the Caribbean, and Bermuda. To facilitate the initiative, the Department of Homeland Security (DHS) expanded on such ongoing ID initiatives as NEXUS, FAST, and SENTRI and adopted a number of different ID solutions, including passport card (PASS Card), Enhanced Driver’s License (EDL), Global Entry and the Enhanced Tribal Card while considering others beyond the costly passport to facilitate commerce, trade, and tourism with Border States. All WHTI IDs employ vicinity-read radio frequency identification (RFID) technology, which has raised privacy concerns. This thesis seeks to join the ongoing civil liberties vs. national security debate through a case study of the EDL on both technological and legal grounds.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAMVA	American Association of Motor Vehicles
ACLU	American Civil Liberties Union
ALA	American Liberty Association
CAC	Common Access Card
CBP	Customs Border Patrol
CDT	Center for Democracy
DES	Data Encryption Standard
DHS	Department of Homeland Security
DMV	Department of Motor Vehicle
EDL	Enhanced Driver's License
EIC	Electronic Electrotechnical Commission
EPC-1	Electronic Product Code Class-1 Generation-1
EPC-2	Electronic Product Code Class-1 Generation-2
EPIC	Electronic Privacy Information Center
EVVE	Electronically Verification of Vital Events
EPIC	Electronic Privacy Information Center
FAST	Fast and Secure Trade
FTC	Federal Trade Commission
FY	Fiscal Year
GAO	Government Accountability Office
GPS	Global Positioning System
ICAO	International Civil Aviation Organization
ID	Identification Document

IRTPA	2004 Intelligence Reform and Terrorism Prevention Act
ISO	International Standards Organization
KB	Kilobytes
KBPS	Kilobytes Per Second
MHz	Megahertz
MRTG	Machine-Readable Travel Documents
MRZ	Machine Readable Zone
NIDS	National Identification System
NTWG	New Technologies Working Group
PASS Card	Passport Card
PASS ID	Providing Additional Security in States Identification
PII	Personally Identifiable Information
PIN	Personal Identification Number
RAM	Random Access Memory
REAL ID	REAL ID Act of 2005
RFID	Radio Frequency Identification
SAVE	Systematic Alien Verification for Entitlements
SENTRI	Secure Electronic Network for Travelers' Rapid Inspection
SSLOV	Social Security On-Line Verification
SN	Serial Number
SSN	Social Security Number
TAG	Technical Advisory Group
TID	Tag Identifier
TSA	Transportation Security Administration
UID	Unique Identifier

U.S.	United States
U.N.	United Nations
WHTI	Western Hemisphere Travel Initiative
Z-Card	United States Merchant Mariner Document

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to acknowledge my wife and children (Samuela and Aurora – they both wanted their names in this thesis) for putting up with a Dad who seemingly can never find the time to be a Dad. Between service and higher education over the past decade…I have obviously been too distant.

I would also like to acknowledge my thesis advisors, Dr. Carolyn Halladay and Dr. Erik Dahl, for their inspiration and hard work cleaning up my gibberish. Without their help on this thesis, it would have been a lot of technical and legal mumbo-jumbo…and still might be.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Members of the National Commission on Terrorist Attacks Upon the United States (more commonly the 9/11 Commission) found U.S. identification documents (IDs)—driver's licenses, passports, birth certificates, etc.—to be critical components in helping the hijackers carry out the 9/11 attacks.[1] In the final wrap-up, the 9/11 investigation members were especially critical of driver's licenses, denoting them "as important as weapons for terrorists,"[2] based on evidence that all but one hijacker had obtained or had fraudulently obtained a driver's license.[3] Importantly, driver's licenses allowed the 9/11 hijackers to mask activities without arousing suspicion. In fact, four of the hijackers were stopped by law enforcement for speeding infractions days to weeks before the devastating attack—and released again, not least because they possessed valid-seeming driver's licenses.[4]

Congress, in response to the 9/11 Commission findings, passed the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA) on December 17, 2004.[5] The act, among many organizational and procedural changes, sought to decrease the exploitability of driver's licenses and thereby increase the capability of systems—law enforcement, Customs Border Patrol (CBP), the Transportation Security Administration (TSA), etc.—that rely on driver's licenses to assure national security and public safety to identify problem driver's licenses and, presumably, thwart terrorist machinations. The act also identified a need to tighten border security, as the 9/11 Commission discovered driver's licenses were often used as proof of identity at border crossings. Congress,

---

[1] Thomas Kean and others, "The 9/11 Commission Report," National Commission on Terrorist Attacks Upon the United States, http://www.9-11commission.gov/report/911Report.pdf (accessed September 18, 2012).

[2] Jean Merserve and Mike Ahlers, "9/11 Commission Members Act to Finally Wrap it Up," CNN, http://cnn.com/2009/US/07/25/new.antiterror.group/index.html (accessed May 6, 2012).

[3] Janice L. Kephart, "Identity and Security: Moving Beyond the 9/11 Staff Report on Identity Document Security," 911securitysolutions.com, http://www.911securitysolutions.com/index.php?option=com_contents&task=view&id=117&Itemid=38 (accessed April 27, 2012).

[4] Ibid.

[5] *Intelligence Reform and Terrorism Prevention Act of 2004*, Public Law 108-796, (2004): 1001.

therefore, inserted into the IRTPA a requirement for the Secretary of Homeland Security, in consultation with the Secretary of State, to find a solution,[6] which later became the Western Hemisphere Travel Initiative (WHTI) on June 1, 2009.[7]

The Department of Homeland (DHS), tasked by the president, responded the driver's license and increase border security requirements identified by the IRTPA. Before groundwork could begin, states and privacy groups mounted strenuous opposition to the act for its imposition on state and individual rights.[8] In light of such concerns, Congress repealed Section 7212 of the IRTPA and enacted the REAL ID Act of 2005 on May 11, 2005, which relaxed the federal mandate and clarified requirements to make driver's licenses acceptable for the "official purposes" of the federal government.[9] Despite relaxing the law, REAL ID continues to receive criticism for many reasons to include, but limited to, its continued imposition on state and individual rights.[10] In other words, REAL ID has done nothing to slake the anxieties of the states'-rights proponents, who increasingly view post-9/11 efforts at streamlining and rationalizing basic security levels as a subterfuge of a national-level government on the march.

In the wake of this opposition to REAL ID, the DHS allowed Washington State to beta-test a voluntary Enhanced Driver's License (EDL) in support of the WHTI on March 23, 2007.[11] The EDL, although informed by REAL ID, is not associated with REAL ID.[12] The program, rather, was tested and subsequently adopted by the DHS to provide states and their citizens a voluntary ID option to support the WHTI that is also less expensive and more convenient than the U.S. passport to expedite land and sea border

---

[6] Ibid.

[7] "Western Hemisphere Travel Initiative." Homeland Security, http://www.dhs.gov/western-hemisphere-travel-initiative (accessed October 21, 2012).

[8] Todd B. Tatelman, *The REAL ID Act of 2005: Legal, Regulatory, and Implementation Issues* (Washington D.C.: Congressional Research Service, 2008.

[9] *REAL ID Act of 2005*, Public Law 109-13, (2005): H.R. 418.

[10] David Williams, "REAL ID Still a REAL Mess," Taxpayers Protection Alliance, http://www.protectingtaxpayers.org/index.php?blog&action=view&post_id=146 (accessed October 21, 2012).

[11] "NASCIO Recognition Award Nomination." NASCIO, http://www.nascio.org/awards/nominations/2009/2009WA2-NASCIO%20AWARD%20INFORMATION%202009%20for%20EDL%20ID%20project_Final.pdf (accessed September 19, 2012).

[12] Tatelman, *The REAL ID Act of 2005: Legal, Regulatory, and Implementation Issues*

crossings between Canada, Mexico, the Caribbean, and Bermuda.[13] Some also have suggested that EDLs more accurately reflect identity and are less "elaborate"[14]—arguably less invasive on state and individual rights—than REAL ID complaint driver's licenses.

The ability of 9/11 terrorists to operate under the radar with U.S.-issued driver's licenses demands not only increased driver's license acquisition standards, as Congress has effected with REAL ID, but also the adoption of the most secure and least invasive ID to assist in preventing a future attack. The EDL has this capability and more. Expressly, the EDL includes radio frequency identification (RFID) technology capable of ID authentication,[15] which is a function of comparing the read-only tag identifier (TID) embedded within the driver's license with federal databases or state Department of Motor Vehicle (DMV) databases via secure systems.[16] EDLs also have the potential to be less invasive, not the least of which is due to the fact that the EDL is a "state" and not a federal ID. Additionally, the technology has the potential to increase interoperability, usability, security, privacy, and reduce identity theft.

Because EDLs more accurately reflect identity, have the potential to be less invasive on state and individual rights, are more secure, offer more capabilities, and provide U.S. citizens with the option to traverse domestic borders without a passport, it stands to reason that all U.S. citizens, as well as federal, state, and local agencies with a counterterrorism mission, should be afforded these benefits rather than only the citizens that may purchase the capabilities from the handful of states that currently authorize the EDL. More importantly, if the EDL is a better tool to protect the homeland from future acts of terrorism and has the potential to be less invasive, REAL ID compliant driver's licenses ought to be replaced or, less painfully, phased out in favor of the EDL. Once complete, this transition could eliminate several, if not all, of the IDs in support of the

---

13 "NASCIO Recognition Award Nomination."

14 Audrey Hudson, "Napolitano Debates REAL ID," *The Washington Times*, February 20, 2009.

15 Colleen Manaher, "Privacy Impact Assessment for the use of Radio Frequency Identification (RFID) Technology for Border Crossings," U.S. Department of Homeland Security, http://foia.cbp.gov/streamingWord.asp?i=45 (accessed September 20, 2012).

16 "Personal Identification - AAMVA North American Standard - DL/ID Card Design." AAMVA, http://www.granddriver.info/uploadedFiles/MainSite/Content/SolutionsBestPractices/BestPracticesModelLegislation(1)/DLIDCardDesignStandard2011.pdf (accessed October, 21, 2012).

WHTI—which also would obviate several National Identification Systems (NIDS). In addition, converting to the EDL will bolster national security by increasing the authentication checks of the EDL while further decreasing privacy threats by eliminating WHTI ID systems utilizing long-range RFID.

Despite the EDL's potential, some states have enacted laws disfavoring or limiting use of the EDL for privacy reasons, which is a consequence of privacy groups that have and continue to strenuously oppose the EDL.[17] Opposition focuses on the EDL's use of vicinity read RFID technology. The technology, as designed, emits unique serial numbers at long range when in proximity of an RFID reader capable of communicating with the RFID tag embedded in the EDL.[18] The concern, thus, is that the unique serial numbers will be intercepted and used for purposes other than what they were intended for or designed to do.[19] The EDL's impact to privacy, thus, must be assessed to determine if these concerns are warranted.

This thesis seeks to analyze the EDL with an eye toward arguing that it represents a better option than REAL ID compliant driver's licenses to ensure national security and civil liberties after the technology is replaced with an encrypted short-range RFID or contact (Smart Card) technology. The analysis begins with background information on the legal and statutory requirements associated with the driver's license, the WHTI, then analysis will turn to the technology and finally privacy issues, and finds, on each front, that the upgraded EDL is the most effective and efficient means of identifying legitimate citizens of the United States at home and at the border.

---

17 "State Statutes Relating to Radio Frequency Identification (RFID) and Privacy." National Conference of State Legislatures, http://www.ncsl.org/issues-research/telecom/radio-frequency-identification-rfid-privacy-laws.aspx (accessed August 22, 2012).

18 "Overview of Enhanced Driver's License." Homeland Security, http://www.cbp.gov/linkhandler/cgov/travel/vacation/enhanced_dl_fs.ctt/enhanced_dl_fs.pdf (accessed May 9, 2012).

19 "Radio Frequency Identification (RFID) Systems." Electronic Privacy Information Center, http://epic.org/privacy/rfid/ (accessed September 18, 2012).

A. A LICENSE TO COMMIT TERRORISM WHILE CURTAILING CIVIL LIBERTIES?

Since 9/11, laws have been enacted and many processes and technological improvements have been made to improve U.S. ID systems. One of the goals is to prevent terrorists from using or abusing "breeder documents"—IDs used to support an individual's identity—to acquire driver's licenses that may later facilitate terror-related activities.[20] (Secure driver's licenses may also prevent crime and illegal immigration, but the primary focus of this thesis is on the prevention of terrorism). After 9/11, there is no argument that terrorists with U.S. issued driver's licenses are more capable of carrying out terror-related activities.[21]

Because U.S. citizens prefer a fractured ID system, Congress and the federal government have limited options other than to influence current ID systems or to create ID systems to address national security issues, either of which will lead to consternation. Anxieties will especially rise when the most pervasive ID in the U.S.—the state driver's license—is influenced based on Big Brother fears of creating a *de facto* national ID. Muddling matters, the driver's license is a state and not a federal function and as such, the Tenth Amendment protects it. Nonetheless, 9/11 demanded change to harden the driver's licenses acquisition process to prevent another "Virginal driver's license scam"[22] or some other fraudulent way to obtain these valuable IDs.

Alongside the impact to the Tenth Amendment, procedures and new technologies adopted for IDs since 9/11 have had an unfavorable impact on civil liberties. REAL ID, for example, has generated Fourth Amendment privacy concerns as a result of an increase in "system" level activity. The law also raised First Amendment concerns as a result of the mandatory facial biometric and the restrictions on commercial air travel. Similarly, the growth in WHTI IDs has, and continues, to receive criticism by privacy groups and many others based primarily on the use of long-range RFID. While doing nothing is not

---

[20] John Mercer, "Breeder Documents," *Keesing Journal of Documents & Identity*, no. 29 (2009): 14-17.

[21] Kephart, *Identity and Security: Moving Beyond the 9/11 Staff Report on Identity Document Security*, 21.

[22] Ibid.

an option, the same 9/11 vulnerabilities for the state driver's license still exist according to a Government Accountability Office (GAO) report dated September 2012.[23]

On top of the latest report to suggest that vulnerabilities still exist in the state driver's license acquisition process, other recent reports suggest that "a flood of high quality counterfeit" driver's licenses are entering the U.S. from abroad, especially China.[24] These counterfeit driver's licenses, in fact, are only detectible under a high-powered electron microscope. The indication, thus, is that the improvements made to the driver's license acquisition processes are working, yet, have created another issue—counterfeiting. Based on the GAO report, however, counterfeit driver's licenses are more likely a result of terrorists or criminals knowing "eyes" are on the system. Nonetheless, the bad news—efforts to improve the acquisition process are meaningless if agents of the law are unable to discern counterfeit driver's licenses.

In order to be alerted in advance of a terrorist attack, the driver's license or the acquisition thereof *must* raise suspicions. If the acquisition process fails, elements imposed—machine-readable zone, full legal name, date of birth, identification number, gold star—do little, if anything, to tip authorities of terrorism. Fortunately, the acquisition process can only improve with time. Unfortunately, process improvements will only evidence an increase of counterfeit driver's licenses. In a busy security environment, say airport security, there is no time to analyze driver's licenses under a high-powered electron microscope to ensure they are not fraudulent.

Based on the concerns above and the fact that states, by law, can design a driver's license in a number of different ways with differing levels of "observable" security features, REAL ID complaint driver's licenses offer little, if any, security from the high-quality counterfeits. What we need is a driver's license that is: less of an impact on the First Amendment; less of an impact on the Fourth Amendment; less of an impact on the Tenth Amendment; decreases the ability to counterfeit driver's licenses commensurate with acquisition hardening; decreases identity theft; increases interoperability to facilitate

---

[23] Daniel Bertoni, *Driver's License Security: Federal Leadership Needed to Address Remaining Vulnerabilities*, United States Government Accountability Office, 2012).

[24] "Call to Action: The Growing Epidemic of Counterfeit Identity Documents and Practical Steps to Combat It." Document Security Alliance, http://www.documentsecurityalliance.com/forms/counterfeit_solutions.pdf (accessed October 21, 2012).

commerce; increases national security; decreases threats to individual privacy; and returns the freedoms to U.S. citizens once known before 9/11, such as having the option to cross borders with a driver's license. Impossible?

B. ENTER THE ENHANCED DRIVER'S LICENSE

The voluntary EDL began as a pilot program in Washington State on March 23, 2007. Washington State officials were concerned that WHTI would affect their robust trade, tourism, and travel relationships with Canada, especially leading up to and during the 2010 Winter Olympics in Vancouver, British Columbia. Officials also believed the high cost of passports would dissuade U.S. citizens from crossing the Washington/British Columbia border.[25] Gaining approval from the DHS, Washington State began offering EDLs with the same technology that supports other WHTI IDs at $15 over the cost of regular driver's license and has continued to issue them ever since.[26]

Based on the success of Washington State's pilot program, the DHS determined the EDL to be an acceptable stand-alone document for entry into the U.S. at all land and sea ports of entry.[27] Approval of the EDL included aspects of security, yet cost and commerce were the driving factors. The "wallet-sized" driver's license–border ID combination is also convenient for those who regularly traverse U.S. land and sea borders.

The WHTI's mild attachment to the driver's license has made it an advanced driver's license tied to REAL ID improvements. The technology in support of the WHTI gives the EDL its distinction from REAL ID compliant driver's licenses. Importantly, the technology offers the capability to authenticate the ID to ensure cardholder identity and, thus, is capable of thwarting the growing epidemic of counterfeit driver's licenses without stifling commerce. Because states retain a degree of control, EDL's could also reduce state and individual rights impacted as a result of REAL ID while at the same time increasing national security.

---

25 "NASCIO Recognition Award Nomination."

26 Ibid.

27 "Overview of Enhanced Driver's License."

The EDL does offer a huge capability to secure the homeland from future acts of terrorism. Civil liberties (privacy) concerns, however, have been raised as a result of the vicinity read RFID technology employed,[28] which could be justified in light of the threat to national security. Because terrorism is a persistent threat, caution is necessary as a new societal expectation for that civil liberty may form as a result of erosion, especially over time, which cannot be undone.[29] As a nation, therefore, it is critical to ensure any course of action that expends civil liberties is necessary and even greater if it lessens Lady liberty's future candlepower.

This thesis argues that once a short-range RFID and/or Smart Card technical solution is adopted, it will not only preserve Lady Liberty's future candlepower, it will brighten her flame by returning civil liberties endangered as a result of REAL ID implementation, while at the same time increasing national security. This result will be accomplished by extrapolating the background on driver's license legal reforms and related matters as well as the EDL's technology and privacy issues in comparison to secure short-range technical solution(s). A final assessment will illustrate how a secure short-range RFID or Smart Card solution is necessary for national security and preserving civil liberties and in a greater sense, liberty.

C. METHODOLOGY

This research is a case study of the EDL using an analytic approach to assess security versus privacy impact. The thesis applies the analysis of proponent and opponent arguments of the security and privacy concerns associated with the use of vicinity read RFID technology employed on EDLs. Conclusions will be formed after considering the legal changes to driver's licenses, subsequent concerns, and the evolution of EDLs along side other WHTI IDs, as well as the technological concerns associated with the use of vicinity read RFID to support the EDL in contrast to alternative solutions and the privacy concerns associated with the current EDL in contrast to alternative solutions. After an

---

[28] "Why the Enhanced Driver's License is Wrong for California." American Civil Liberties Union of Northern California, https://www.aclunc.org/issues/technology/asset_upload_file944_8427.pdf (accessed August 27, 2012).

[29] Joshua Levy, "Towards a Brighter Fourth Amendment: Privacy and Technology Change," *Virginia Journal of Law & Technology* 16, no. 4 (Winter, 2011): 504.

assessment of the EDL to support an argument for a change in technology, final analysis of information will result in a recommendation(s) that best balances national security alongside state and individual rights and in particular, privacy.

D. THESIS OVERVIEW

This thesis begins with a background chapter (II) with the following subsections: In The Cards: Identification Since 9/11; The 2004 Intelligence Reform and Terrorism Prevention Act; The REAL ID Act of 2005; The Western Hemisphere Travel Initiative; and The Take Away. The focus of Chapter II is the "who, what, when, why, and where" of driver's license standards beginning with the attacks on 9/11 leading up to the subsequent use of RFID-enabled driver's licenses for border security. Emphasis will be placed on issues associated with the REAL ID, particularly, the concerns to state and individual rights, and the problems and limitations of the REAL ID to form the arguments for subsequent chapters related to the underlying privacy vs. national security debate.

Chapter III will analyze the technological concerns associated with EDL's vicinity read RFID technology with the following subsections: A Short History on RFID For Border Control; the Technology Argument in a Nutshell; the RFID Basics for Identity Documents; Technological Concerns for the RFID-Enabled EDL; a Technology Comparison of Identity Documents; Other Technological Considerations; and the Take Away and Solution. The analysis of ID technologies (alternatives to vicinity read RFID technology, barcode technology, magnetic swipe technology, and Smart Card technology) will also assist the Chapter V assessment and recommendations in Chapter VI.

Chapter IV will analyze the privacy concerns associated with the EDL with the following subsections: The Privacy and National Security Debate; Contextual Evaluation of the Current EDL; and Does the Improved EDL Address Privacy Concerns? The analysis of the privacy concerns will assess both the vicinity read RFID against the technologies identified in Chapter III that were identified as superior. Importantly, analysis will further support a need for a secure solution and assist in making assessments in Chapter V and recommendations in Chapter VI.

Chapter V will provide a full assessment of all information gathered with following subsections: Political Assessment; Economic Assessment; Limitations Assessment; Technological Assessment; and Privacy Assessment. Combined, the assessments will showcase the optimal solution and form the recommends for Chapter VI. The objective is to demonstrate that the EDL not only benefits all federal, state, and local officials in the quest to prevent another devastating attack, but also provides the optimum solution to preserve our cherished civil liberties.

II. BACKGROUND

9/11 revealed that state driver's licenses are a national security imperative, which was a consequence of the role they played in support of the 9/11 hijackers prior to their dastardly act. The gap in national security demanded action by Congress. States and privacy groups, however, continue to challenge Congressional actions and the DHS responses. Often options to reduce pushback are not apparent. This chapter will lay the groundwork in support of an argument that the EDL, with necessary modifications to technology, is a more secure, efficient, and less invasive solution to REAL ID compliant driver's licenses.

A. IN THE CARDS: IDENTIFICATION SINCE 9/11

The investigation into 9/11 revealed that 18 of the 19 hijackers had obtained driver's licenses from various states, and at least six were used as valid ID to board the aircraft that rammed the World Trade Center buildings and the Pentagon. Significantly, seven of these driver's licenses were fraudulently obtained from the State of Virginia, and 14 of the 18 were duplicates, that is, the 9/11 hijackers obtained more than one valid state driver's license.[30] The driver's licenses, thus, allowed the hijackers to make their plans and prepare their attack without arousing suspicion, which is why the 9/11 Commission members deemed driver's licenses, and the IDs to acquire them, to be as important as weapons to terrorists.[31]

From the evidence, the 9/11 Commission stated: "Secure identification should begin in the United States. The federal government should set standards for the issuance of birth certificates and sources of identification, such as driver's licenses. Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether

---

[30] Kephart, *Identity and Security: Moving Beyond the 9/11 Staff Report on Identity Document Security*, 21.

[31] Merserve and Ahlers, *9/11 Commission Members Act to Finally Wrap it Up*

they are terrorists."[32] This observation echoed the 2003 Second Report of the Markle Foundation Task Force, which argued that collateral improvements to U.S. IDs, particularly driver's licenses, be made to enhance security. Specifically, the Markle report concluded, the federal government should: 1) assist in making state driver's licenses and other state-issued ID documents more reliable; and 2) study whether biometric or cryptographic technologies can increase reliability while addressing privacy concerns.[33]

The attacks on 9/11 served as a wake-up call to improve standards for commonly issued U.S. driver's licenses and such other forms of ID as birth certificates and passports and to increase the capability of systems that rely on IDs to safeguard the national, economic security and public safety of the United States, notably border security, law enforcement, intelligence, and the DMV. Congress responded by enacting two laws, IRTPA and the REAL ID Act of 2005, which established federal requirements for IDs and tightened the requirements, procedures and processes associated with IDs. These acts gave rise to the changes to driver's licenses and, thus, the subsequent issues, limitations and concerns.

B. THE 2004 INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT

The first effort on driver's license and personal IDs came in the form of the IRTPA, sponsored by Senator Susan Collins (R-Maine). Congress passed the act on December 17, 2004, in response to the 9/11 Commission recommendations. Although the law covers many aspects, the following items in Section 7209(a) were linked to IDs: 1) existing identification procedures allow many individuals to enter the U.S. by showing minimal identification or without showing any identification; 2) the planning for the terrorist attacks of 9/11 demonstrates that terrorists study and exploit U.S. vulnerabilities; and 3) additional safeguards are needed to ensure that terrorists cannot enter the United States.[34] Section 7209(b)(1) of the IRTPA mandated that by January 1, 2008:

---

[32] Kean and others, *The 9/11 Commission Report*, 585-390.

[33] "Creating a Trusted Information Network for Homeland Security: Second Report of the Markle Foundation Task Force," *Markle Foundation*, 2003.

[34] Collins, *Intelligence Reform and Terrorism Prevention Act of 2004*, 1001-8404.

> The Secretary of Homeland Security, in consultation with the Secretary of State, shall develop and implement a plan as expeditiously as possible to require a passport or other document, or combination of documents, deemed by the Secretary of Homeland Security to be sufficient to denote identity and citizenship for all travel into the United States by United States citizens and by categories of individuals for whom documentation requirements have previously been waived under section 212(d)(4)(B) of the Immigration and Nationality Act. (8 U.S.C. 1182(d)(4)(B))[35]

Section 7212 of the IRTPA also established federal standards for driver's licenses and personal ID cards and indicated that no federal agency would accept a driver's license or personal ID card two years after a date established by the Secretary of Transportation (no less than eighteen months from enactment of the IRTPA unless minimum federal standards were met). A two-year extension was afforded if a state was making a reasonable attempt to meet the deadline. Section 7212(b)(2) stipulated the following minimum standards for states:[36]

- Standards for documentation required as proof of identity and an applicant for a driver's license or personal identification card
- Standards for the verifiability of documents used to obtain a driver's license or personal identification card
- Standards for the processing of applications for driver's licenses and personal identification cards to prevent fraud
- Standards for information to be included on each driver's license or personal identification card, including: the person's full legal name; the person's date of birth; the person's gender; the person's driver's license or personal identification card number; a digital photograph of the person; the person's address of principle residence; and the person's signature
- Standards for common machine-readable identity information to be included on each driver's license or personal identification card, including defined minimum data elements
- Security standards to ensure that driver's licenses and personal identification cards are: resistant to tampering, alteration, or counterfeiting; and capable of accommodating and ensuring the security of a digital photograph or other unique identifier

[35] Ibid.

[36] Ibid.

- A requirement that a State confiscate a driver's license or personal identification card if any component or security feature of the license or identification card is compromised

The requirements of Section 7212 were not well received by states and privacy groups. The arguments, in general, were that the IRTPA interfered with the right to grant driver's licenses to certain categories of individuals—for instance, legal aliens—unfairly mandated a single uniform design, failed to include procedures to protect the privacy rights of individual applicants, and did not make use of negotiated rulemaking pursuant to the Administrative Procedure Act.[37] Congress, in response, repealed Section 7212 and enacted the REAL ID Act of 2005.

C. THE REAL ID ACT OF 2005

Congress enacted the REAL ID Act of 2005 on May 11 of the same year as supplemental bill (Division B) to the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief (P.L. 109–13). The law, sponsored by James Sensenbrenner (R-Wisconsin), repealed section 7212 of the IRTPA to clarify federal ID standards and relax the federal mandate inferred by the IRTPA.[38]

Unlike the IRTPA, REAL ID clearly does not demand compliance. Noncompliant state-issued driver's licenses and ID cards, however, must be marked and feature a unique design or color to alert federal agencies or law enforcement personnel that they do not comply with the REAL ID guidelines. Either way, driver's license data must still be electronically accessible by all other states and contain such information as drivers' histories, including violations, suspensions, and points against the license. The law also stipulates that noncompliant IDs are insufficient for "official purposes," to include such activities as boarding federally regulated commercial aircraft or entering federally controlled facilities.[39] States, thus, have a significant incentive to make their licenses accord with REAL ID standards.

Driver's license and identity document standards are listed under Section 202(b), Minimum Document Requirements; Section 202(c), Minimum Issuance Standards; and

---

[37] Tatelman, *The REAL ID Act of 2005: Legal, Regulatory, and Implementation Issues*

[38] Sensenbrenner, *REAL ID Act of 2005*, H.R. 418-H.R. 1268.

[39] Ibid.

Section 202(d), Other Requirements.[40] The minimum document requirements for federal purposes are as follows:

- The person's full legal name
- The person's date of birth
- The person's gender
- The person's driver's license number or identification card number
- A digital photograph of the person
- The person's principle address
- The person's signature
- Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes
- A common machine-readable technology, with defined minimum data elements

The minimum issuance requirements are as follows:

- A photo identity document, except that a non-photo identity document is acceptable if it includes both a person's full legal name and date of birth
- Document showing the person's date of birth
- Proof of a person's social security account number or verification that the person is not eligible for a social security number
- Documentation showing the person's name and address of principle residence
- Evidence of lawful status
- Other requirements include:
- Employ technology to capture digital images of identity source documents so that the images can be retained in electronic storage in a transferable format
- Retain paper copies of source documents for a minimum of 7 years or images of source documents presented for a minimum of 10 years
- Subject each person applying for a driver's license or ID card to mandatory facial image capture
- Establish an effective procedure to confirm or verify a renewing applicant's information

[40] Ibid.

- Confirm with the Social Security Administration a social security account number presented by a person using the full social security number and resolve discrepancies
- Refuse to issue a driver's license or ID card to a person holding a driver's license issued by another State without confirming that the person is terminating or has terminated the driver's license
- Ensure the physical security of locations where driver's licenses and ID cards are produced and the security document materials and papers from which driver's licenses and ID cards are produced
- Subject all persons authorized to manufacture or produce driver's licenses and ID cards to appropriate security clearance requirements
- Establish fraudulent documentation recognition training programs for appropriate employees engaged in the issuance of driver's licenses and ID cards
- Limit the period of validity of all driver's licenses and ID cards that are not temporary to a period that does not exceed eight years

1. REAL Concerns

According to REAL ID, federal requirements were to be imposed three years from the date of enactment, May 11, 2008.[41] The implementation timeline, however, has been twice extended and is currently January 15, 2013.[42] The latest deadline is unlikely to be achieved despite significant progress. Much has to do with funding, though state and privacy group opposition has been a significant factor. Major concerns about the law include its constitutionality—states' rights under the Tenth Amendment, freedom of religion (mandatory facial image capture) under the First Amendment—undue restrictions on commercial air travel, and inadequate federal funding to impose the law per the Unfunded Mandate Reform Act.[43]

More controversially, many opponents believe that the law creates a *de facto* national ID.[44] The national ID concern is, in large part, a consequence of Section 202(d)(12), which requires DMV databases to be electronically accessible to all states (in

41 Ibid.

42 Janice L. Kephart, "REAL ID Implementation Annual Report: Major Progress made in Securing Driver's License Issuance Against Identity Theft and Fraud," *Backgrounder* (February, 2012): 11.

43 Tatelman, *The REAL ID Act of 2005: Legal, Regulatory, and Implementation Issues*

44 Ibid.

response to the evidence that hijackers acquired driver's licenses from multiple states). In fact, more than twenty-five privacy groups continue to oppose the law for this and other privacy concerns, to include, but not limited to, the American Civil Liberties Union (ACLU), American Liberty Association (ALA), Center for Democracy and Technology (CDT), Electronic Privacy Information Center (EPIC), and the Rutherford Institute.[45]

Privacy advocates are also concerned that Section 202(d)(12) will increase privacy risks, as thousands of DMVs will have access to millions of Americans personal identifiable information (PII) that place them at greater risk of identity theft if the system is compromised.[46] This danger is compounded by the requirement to capture source documents (Section 202(d)(2)).[47] Many DMVs, however, are increasingly utilizing the Electronic Verification of Vital Events (EVVE) system to verify birth certificates, Social Security On-Line Verification (SSLOV) to verify Social Security Numbers (SSNs), and Systematic Alien Verification for Entitlements (SAVE) system that could conceivably cut down on source documents the DMV captures and stores electronically.[48]

Another controversial matter concerns the mandatory facial biometric in Section 202(d)(3). It is not required to be stored on the driver's license, but for some, it smacks of domestic intelligence and social control.[49] Facial biometric is largely considered precognitive (guilty until proven innocent), while other biometrics, such as fingerprints, are generally not (innocent until proven guilty). The concern is that civil liberties, particularly privacy, could be compromised as a result of unwarranted surveillance, tracking, linking or the transfer of biometric data between databases, and the proliferation of biometrics on databases.[50]

---

45 "Secure Identification: The REAL ID Act's Minimum Standards for Driver's Licenses and Identification Cards." http://judiciary.house.gov/hearings/printers/112th/112-103_73416.PDF (accessed September 18, 2012).

46 Ibid.

47 Sensenbrenner, *REAL ID Act of 2005*, H.R. 418-H.R. 1268.

48 Kephart, *REAL ID Implementation Annual Report: Major Progress made in Securing Driver's License Issuance Against Identity Theft and Fraud*, 11.

49 "Biometrics: Who's Watching You?" Electronic Frontier Foundation, https://www.eff.org/wp/biometrics-whos-watching-you (accessed September, 20, 2012).

50 Ibid.

2. REAL Limitations

Title 6 CFR 37.15, in support of REAL ID, titled "Physical security features for the driver's license or identification card" provides a need for driver's licenses and ID cards to be designed "to deter forgery and counterfeiting, promote an adequate level of confidence in the authenticity of cards, and facilitate detection of fraudulent cards."[51] Specifically, they must not be capable of being reproduced using technologies that are commonly used and made available to the general public; and they must contain a well-designed, balanced set of features that are effectively combined to provide multiple layers of security.[52]

To comply with 6 CFR 37.15, states must employ a minimum of three levels of security. Level 1 involves the detection of fraudulent IDs by a cursory visual examination and without tools or aids. Examples include a holographic feature, tactile engraving (data burnt onto the ID), complex background, tactile or raised feature, or a laser-engraved photograph. Level 2 involves the detection of fraudulent IDs through examination by trained inspectors with simple equipment—perhaps an ultraviolet light or a magnifying glass. Level 3 involves the detection of fraudulent IDs through examination by forensic specialists of items only seen with high magnification or an electron microscope.[53]

The major limitation of REAL ID compliant driver's license, thus, is the lack of a common denominator. That is to say, states can comply with the REAL ID's physical security requirements in many ways. A TSA agent, law enforcement officer, or other official cannot be expected to memorize or discern all of the designs and security features each state imposes, especially in a busy security environment like airport security. Moreover, each state often has three or more types of IDs. Just the State of Michigan, for example, has a normal ID card, an enhanced ID card, a normal driver's license, the EDL,

---

51 "Title 6 - Homeland Security 6 CFR Part 37: 37.15 Physical Security Features for the Driver's License Or Identification Card." Department of Homeland Security, http://uscis.gov/ilink/docView/6CFR/HTML/6CFR/0-0-0-1/0-0-0-4972/0-0-0-5202.html (accessed September 20, 2012).

52 Ibid.

53 Marty Kenner, Bruce Wilson and Steve Rhyner, "U.S. Driver's Licenses: Addressing the Potential Vulnerabilities," 3M, http://solutions.3m.com/3MContentRetrievalAPI/BlobServlet?lmd=1329168842000&locale=en_WW&assetType=MMM_Image&assetId=1319220855046&blobAttribute=ImageFile (accessed September, 20, 2012).

as well as different IDs with the design turned on its side to indicate that the bearer is younger than 21 (see Figure 11). When all 56 jurisdictions are combined, thus, it does not take a perfect counterfeit driver's license or ID card to undermine security, particularly those systems that rely solely on visual indicators and are unfamiliar with all security measures.

Figure 1. Michigan Driver's Licenses & ID Cards. (From TOKENWORKS, Department of State, and Michigan Secretary of State respectively.)

Another major limitation is a result of the evidence revealing that only Level 3 offers a credible level of security that, again, requires an electron microscope.[54] According to the Document Security Alliance: "There is a growing sophistication in high quality counterfeit driver's licenses and state issued IDs, some of which are produced overseas and others in major metropolitan areas by professional criminals. In particular, there is a virtual flood of low cost, high quality counterfeits being shipped by the tens of thousands from China…"[55] Speculation for the increase in high-quality counterfeits is a consequence of REAL ID efforts to harden the driver's license acquisition process or the fear of knowing the system is more heavily monitored. Irrespective, it is impractical for agents of the law in the course of normal duty to discern a Level 3 abnormality.

---

54 Matt Markovich, "'Near-Perfect" Fake IDs Pose Law Enforcement Challenge," Komonews, http://www.komonews.com/news/local/Near-perfect-fake-IDs-pose-law-enforcement-challenge-153736705.html (accessed October 21, 2012).

55 "Call to Action: The Growing Epidemic of Counterfeit Identity Documents and Practical Steps to Combat It."

3. REAL Status

Final Rule 5–08, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes (73 FR 5271), published on January 29, 2008, addressed some of the major concerns of REAL ID aired during a 60-day public comment window that received 21,000 comments to the DHS and subsequently codified in subsections of 6 CFR Part 37.[56] Of the many notable concessions, the following are considered significant changes:

- The DHS is working with the American Association of Motor Vehicle Administrators (AAMVA) network for state-to-state verification of IDs, which operates on an end-to-end encrypted network not tied to the Intranet.
- The use of the AAMVA network supports verification of SSNs and birth certificates and the application systems that enable states to query SSOLV and EVVE securely.
- The DHS relaxed the demand to "refuse to issue a driver's license or identification card to a person holding a driver's license issued by another state without confirmation…" and now only encourages the policy of "one driver, one license" and/or a reasonable attempt to verify.
- Driver's licenses that are REAL ID-complaint must conform to the "one driver, one license" concept.
- The DHS deleted proposed card design standards, and replaced the language with the need for states to provide the DHS with the designs applied to resist compromise of the ID.

The latest 2012 report on the implementation of the REAL ID indicates that 53 of 56 state and territorial jurisdictions have embraced REAL ID principles; 36 are "materially or substantially materially" compliant. Moreover, only three jurisdictions, two of which are territories, have not embraced REAL ID principles.[57] Notably, 39 states have proposed or enacted legislation to urge Congress to respect state rights and the

---

[56] "Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes [73 FR 5271][FR 5-08]." Office of the Secretary, DHS, http://www.uscis.gov/ilink/docView/FR/HTML/FR/0-0-0-1/0-0-0-145991/0-0-0-165820/0-0-0-176819.html

[57] Kephart, *REAL ID Implementation Annual Report: Major Progress made in Securing Driver's License Issuance Against Identity Theft and Fraud*, 11.

privacy of driver's license applicants.[58] Yet, all 56 jurisdictions have accepted a portion of the $263 million in total federal grants since 2007 to support aspects of REAL ID, a strong indication that all states and territories will eventually become REAL ID compliant.[59]

On March 21, 2012, Representative Sensenbrenner expressed concerns over the DHS's commitment to the REAL ID.[60] His comments focused on the lack of manpower allocated to the Office of State-Issued Identification Support within the Office of Policy; the fact that the DHS had not published grant guidance for FY12; the fact that the DHS had not notified the U.S. public about the impeding deadline set for REAL ID, and a latent willingness to support the proposed PASS ID Act.[61] The DHS, however, contends that significant progress has been accomplished in the face of strong opposition to the law.

D. THE WESTERN HEMISPHERE TRAVEL INITIATIVE

Before 9/11 and for several years thereafter, it was possible for U.S. citizens to cross into Canada, Mexico, the Caribbean, and Bermuda with a state driver's license and sometimes with no ID at all. Based on the 9/11 Commission report, Congress recognized a need to tighten security at the border and, with IRTPA, signed into law a requirement for the DHS to develop a solution by January 1, 2008.[62] Recognizing implementation timeline issues, the President signed into law the Department of Homeland Security

---

58 "REAL ID State Legislation Database." National Conference of State Legislatures, http://www.ncsl.org/issues-research/transport/real-id-state-legislation.aspx (accessed September 18, 2012).

59 Kephart, *REAL ID Implementation Annual Report: Major Progress made in Securing Driver's License Issuance Against Identity Theft and Fraud*, 11.

60 "Secure Identification: The REAL ID Act's Minimum Standards for Driver's Licenses and Identification Cards." 104-7.

61 Providing for Additional Security in States Identification Act of 2009, or PASS ID Act, sought repeal title II of the REAL ID Act of 2005 and amend title II of the Homeland Security Act of 2002 to better protect the security, confidentiality, and integrity of personally identifiable information collected by States when issuing driver's licenses and identification documents. The bill, however, met heavy resistance as it replaced the substance of REAL ID by deleting identity verification and document authentication and replacing them with what is, for the most part, the status quo in most states, or standards that are less rigorous than those now in place.

62 Collins, *Intelligence Reform and Terrorism Prevention Act of 2004*, 1001-8404.

Appropriations Act of 2007 on October 2, 2006, amending section 7209 of the IRPTA to establish June 1, 2009, as the deadline for implementing travel requirements.[63]

On April 2, 2008, DHS established a joint final rule (73 FR 18384), effective June 1, 2009, to implement WHTI.[64] All travellers crossing borders, to include the land or sea borders into the U.S. from Canada, Mexico, the Caribbean and Bermuda, thus, must meet ID requirements. Valid U.S. IDs include: U.S. Passport; Passport Card; Enhanced Driver's License; Trusted Traveller Program Card (i.e., NEXUS, SENTRI, FAST, and Global Entry); U.S. Military ID card with official orders; U.S. Merchant Mariner document (Z-Card) when travelling in conjunction with official maritime business; and FM I-872 American Indian Card/Enhanced Tribal Card (see Table 1).[65]

---

63 "Documents Required for Travelers Departing from Or Arriving in the United States at Air Ports-of-Entry from within the Western Hemisphere." *Federal Register* 71, (November 24, 2006): 68412.

64 "Western Hemisphere Travel Initiative: Designation of Enhanced Driver's Licenses and Identity Documents Issued by the States of Vermont and Michigan and the Provinces of Quebec, Manitoba, British Columbia, and Ontario as Acceptable Documents to Denote Identity and Citizenship." The Federal Register, www.federalregister.gov/articles/2009/05/29/E9-12513/western-hemisphere-travel-initiative-designation-of-enhanced-drivers-licenses-and-identity-documents (accessed May 11, 2012).

65 "Western Hemisphere Travel Initiative: Land and Sea Travel Document Requirements." U.S. Customs and Border Protection, http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/travel/whti_state_factsheet.ctt/whti_state_factsheet.pdf (accessed May 11, 2012).

	PRICE	AIR	LAND	SEA	TECH	WHTI	DATA
REAL ID Driver's License	$25 Avg.	Domestic Use Only	Domestic Use Only	No	Barcode	No	PII/SN
EDL	$55 Avg.	Domestic Use Only	All WHTI Borders	All WHTI Borders	Vicinity Read RFID	Yes	SN
PASS ID	$55	No	All WHTI Borders	All WHTI Borders	Vicinity Read RFID	Yes	SN
SENTRI	$122.50	No	Specific WHTI Locations	No	Vicinity Read RFID	Yes	SN
NEXUS	$50	No	Specific WHTI Locations	No	Vicinity Read RFID	Yes	SN
FAST	$50	No	Specific WHTI Locations	No	Vicinity Read RFID	Yes	SN
GLOBAL ENTRY	$100	Approved Locations	Specific WHTI Locations	No	Vicinity Read RFID	Yes	SN
E-PASSPORT	$140	Global Use	Global Use	Global Use	Passive Read RFID	No	PII/SN
MILITARY ID	N/A	All WHTI Borders w/Orders	All WHTI Borders w/Orders	All WHTI Borders w/Orders	Contactless Smart Card	No	PII/SN
ETC	$30	No	All WHTI Borders	All WHTI Borders	Vicinity Read RFID	Yes	SN

Table 1. Border ID General Comparison Chart[66]

1. U.S. Passport

The U.S. passport (see Figure 1) is the standard border-crossing ID recognized at all air, land, and sea ports of entry (not a WHTI ID, but it is border ID). It currently costs

[66] [Note SN=serial number]

$140 for adults and $80 for minors, plus an additional $25 for first-time applicants.[67] Since August of 2007, all U.S. passports utilize passive-read (short-range) RFID technology—e-passports—as a result of the standards set by the International Civil Aviation Organization (ICAO) of the United Nations (U.N.) to facilitate border security.[68] Data stored on the RFID technology includes what is visually displayed on the data page of the passport, a biometric identifier in the form of a digital facial image, a unique number, and digital signature to protect the stored data and to prevent counterfeiting.[69]

Figure 2. Passport, United States of America. (From Translators and Christians.)

2. Trusted Traveler

"Trusted Traveler" programs allow expedited border crossing or security searches for regular border-crossers who agree to provide certain personal information to the government in advance through the application process.[70] The four WHTI Trusted Traveler programs for low-risk travelers are NEXUS, the Secure Electronic Network for Travelers' Rapid Inspection (SENTRI), Free and Secure Trade (FAST), and Global Entry

---

67 "Passport Fees." U.S. Department of State, http://travel.state.gov/passport/fees/fees_837.html (accessed September 19, 2012).

68 "The U.S. Electronic Passport." U.S. Department of State, http://travel.state.gov/passport/passport_2498.html (accessed September 19, 2012).

69 "The U.S. Electronic Passport Frequently Asked Questions." U.S. Department of State, http://travel.state.gov/passport/passport_2788.html (accessed September 19, 2012).

70 "Trusted Traveler Programs." Homeland Security, http://www.dhs.gov/trusted-traveler-programs (accessed October 21, 2012).

(see Figure 2).[71] NEXUS cards are designed for prescreened Canadian and U.S. citizens on specified northern-border locations and currently cost $50 per person.[72] SENTRI cards are similar to NEXUS cards for specified locations on the southern border at a current cost $122.25.[73] FAST cards are also similar to NEXUS and SENTRI cards, yet can be found at specified locations on both the northern and southern borders at a current cost of $50; most FAST card holders are truckers who cross the borders regularly.[74] Global Entry cards are good for SENTRI and NEXUS lanes as well as expedited domestic air travel with certain airlines and at particular locations, at a current cost of $100.[75] All Trusted Traveler programs have a dedicated commuter lane(s) to expedite travel that is further facilitated by vicinity read (long-range) RFID technology embedded within the IDs that emits a unique ID number.[76]

Figure 3. SENTRI, NEXUS, FAST, & Global Entry. (From U.S. Customs Border Protection.)

71 "Trusted Traveler Programs." Customs Border Patrol, http://www.cbp.gov/xp/cgov/travel/trusted_traveler/ (accessed September 19, 2012).

72 "NEXUS Eligibility and Fees." Customs Border Patrol, http://www.cbp.gov/xp/cgov/travel/trusted_traveler/nexus_prog/nexus_eligibility.xml (accessed September 19, 2012).

73 "SENTRI Program Description." Customs Border Patrol, http://www.cbp.gov/xp/cgov/travel/trusted_traveler/sentri/sentri.xml (accessed September 19, 2012).

74 "FAST Fact Sheet." Customs Border Patrol, http://www.cbp.gov/xp/cgov/travel/trusted_traveler/fast/fast_fact_sheet.xml (accessed September 19, 2012).

75 "Participation: Risk Based Security Initiative." Transportation Security Administration, http://www.tsa.gov/what_we_do/participation.shtm (accessed September 19, 2012).

76 "Western Hemisphere Travel Initiative." Customs Border Patrol, http://www.getyouhome.gov/html/rfid/RFID.html (accessed September 19, 2012).

3. PASS Card and Enhanced Driver's License

The passport card (PASS card) and EDL are IDs approved for the WHTI (see Figure 3). Unlike the Trusted Traveller programs, PASS cards and EDLs can be used to enter the U.S. from all land-border crossings between the U.S. and Canada, Mexico, the Caribbean, and Bermuda as well as sea ports-of-entry (not approved for international travel by air).[77] PASS cards currently cost $55 for adults and $40 for minors under the age of 16. Renewal of card costs $30.[78] EDLs, unlike PASS cards, are not available to all citizens. At this time only the residents from Michigan, New York, Vermont, and Washington have the option, though other states, like Minnesota, are making arrangements.[79] The average cost of an EDL is $30 over the cost of a regular driver's license (Michigan, $45[80]; New York, $30[81]; Vermont, $25[82]; Washington State, $35[83]; Minnesota passed legislation indicating $15[84]). Both the PASS card and EDL employ vicinity-read RFID technology that emits a unique ID number to facilitate border security.[85]

Unlike any of the other WHTI IDs, to include the PASS card, states that desire to issue EDLs to U.S. citizens must enter into an agreement with the DHS.[86] States can

---

77 "Western Hemisphere Travel Initiative: Designation of Enhanced Driver's Licenses and Identity Documents Issued by the States of Vermont and Michigan and the Provinces of Quebec, Manitoba, British Columbia, and Ontario as Acceptable Documents to Denote Identity and Citizenship," 7.

78 "U.S. Passport Card." U.S. Department of State, http://travel.state.gov/passport/ppt_card/ppt_card_3926.html (accessed September 19, 2012).

79 "Enhanced Driver's Licenses: What are they?" Homeland Security, http://www.dhs.gov/enhanced-drivers-licenses-what-are-they (accessed September 19, 2012).

80 "Driver's License & State ID: Enhanced Driver's License Fee Chart." Michigan Department of State, http://www.michigan.gov/sos/0,1607,7-127-1627_8669_9040-213056--,00.html (accessed September 19, 2012).

81 "FAQs about Enhanced Driver's Licenses and Enhanced Non-Driver Photo ID Cards." New York Department of Motor Vehicles, http://www.dmv.ny.gov/edl-faqs.htm (accessed September 19, 2012).

82 "License/Permit/ID Fees: Payment Information." Vermont Department of Motor Vehicles, http://dmv.vermont.gov/fees/license-permit-id (accessed September 19, 2012).

83 "Driver Licensing Fees." Washington State Department of Licensing, http://www.dol.wa.gov/driverslicense/fees.html (accessed September, 19, 2012).

84 Tom Saxhaug, "News Release: Enhanced Driver's License Bill Passes Legislature," Minnesota Senate, http://www.senate.mn/members/member_pr_display.php?ls=&id=3396 (accessed September 19, 2012).

85 "Western Hemisphere Travel Initiative."

86 "Western Hemisphere Travel Initiative: Land and Sea Travel Document Requirements," 2.

choose either a "push" or "pull" method to give CBP agents the ability to verify cardholder identity and to authenticate the driver's license. In the push method, states transfer data to a secure database controlled by the DHS. In the pull model, however, "issuing states store their data in their own database and CBP retrieves the data at time of presentation at a border crossing via NLETS."[87] NLETS is nonprofit organization that offers a secure and audited system, "owned by the States," for the exchange of law enforcement information.[88]

To obtain an EDL, U.S. citizens are required show proof of the following: 1) a valid Social Security Number; 2) source documents, such as a birth certificate, to prove U.S. citizenship; 3) identity verification through a photo document; and 4) proof of residency. In addition, they must have a personal interview with a licensing representative to verify the applicant's information.[89] Of note, the only tangible procedural difference between REAL ID and the EDL for U.S. citizens is the personal interview.

According to Janet Napolitano, Secretary of Homeland Security, "enhanced driver's licenses give confidence that the person holding the card is the person who is supposed to be holding the card, and it's less elaborate than REAL ID."[90] All EDLs issued to date, however, comply and are expected to comply with the document and issuance requirements of REAL ID and as such, are more elaborate than REAL ID compliant driver's licenses. Expressly, EDLs include RFID technology that emits a unique ID number capable of interfacing with CBT systems at long read range, which allows them to interface with state or federal databases to validate the identity of the cardholder and authenticate the EDL.

Although EDLs comply with REAL ID document and issuance requirements, not all elements of REAL ID have been satisfied by some of the state's issuing EDLs. Washington State, for example, passed legislation to oppose REAL ID based on the

---

87 "Personal Identification - AAMVA North American Standard - DL/ID Card Design."

88 "Mission & Vision." NLETS, https://www.nlets.org/mission-vision (accessed October 21, 2012).

89 "Get Your EDL/EID." Washington State Department of Licensing, http://www.dol.wa.gov/driverslicense/edlget.html (accessed May 12, 2012).

90 Hudson, *Napolitano Debates REAL ID*

privacy concerns.[91] The privacy concerns of vicinity read RFID-enabled EDLs, however, are just as prevalent. Concerns stem not only from privacy advocates, but also from members of Congress, RFID manufacturers, scholars, and many U.S. citizens.[92]

Figure 4. Passport Card & Enhanced Driver's License. (From U.S. Department of State and *The New York Times.*)

4. Other Credentials

Other credentials accepted for border crossings are the U.S. Military ID with official orders, the Z-card, and the FM I-872 American Indian Card or Enhanced Tribal Card (see Figure 4). Although the military ID card has contact technology (i.e., smart chip without RFID), it is not used as a means of verification or authentication and as such, military orders provide a means of verification. Z-cards also do not employ RFID technology, however, they are being phased out. For Native Americans, FM I-872 American Indian Card will suffice until supplanted by the RFID-enabled Enhanced Tribal Card (ETC).[93]

---

91 "Washington, Hew Hampshire, and South Carolina Oppose Real ID." North Country Gazette, http://www.northcountrygazette.org/articles/2007/040807SixOppose.html (accessed September 19, 2012).

92 "Card Format Passport; Changes to Passport Fee Schedule." *Federal Register* 72, no. 249 (December 31, 2007, 2007b): 74170.

93 "WHTI: Special Groups." Customs Border Patrol, http://www.getyouhome.gov/html/lang_eng/eng_sa.html (accessed September 19, 2012).

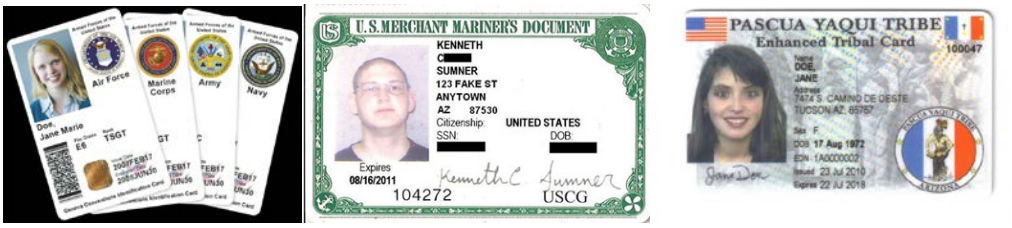

Figure 5. Military ID, Z-Card & Enhanced Tribal Card. (From Spousebuzz, United States Coast Guard, and U.S Department of Homeland Security.)

E. THE TAKE-AWAY

State driver's licenses are valuable IDs for terrorists to disguise activity and/or to assimilate into society; thus, it is necessary to ensure the acquisition process is secure to assure identity of U.S. citizens and that agents of the law who rely on state driver's licenses are able to safeguard national security and public safety. Yet, levying change upon the state driver's licenses has been precarious as it invigorated and continues to stimulate anxiety, particularly for state rights, individual rights, privacy concerns, and *de facto* ID concerns. The difficulties have led to additional ID fracturing and growth in PII in federally controlled, but secure, database systems to support ID requirements.

Countermeasures to ensure ID security are capable of preventing terrorists from producing a counterfeit driver's license at Level 3, but inadequate for everyday use when high-quality counterfeits are capable of defeating Level 1 and Level 2 security. Thus, a need exists for an interoperable, secure, and quick system to reduce the ability to counterfeit a driver's licenses with little or no impact to commerce. The RFID solutions used in border IDs, particularly the EDL, ostensibly offers the capably to fill this gap.

The EDL provides proof that it is possible to use authentication technology for all drivers' licenses, which may alleviate the pressure to develop alternative ID solutions for border security that could still remain optional for that purpose. The EDL also indicates that the need for a large federal database is unnecessary, as it is possible to satisfy both state and federal needs using the "pull" model that is both state owned and operated. The EDL, however, has generated privacy concerns due to using the same long-range technology for other border ID solutions; hence, a need to extrapolate the technology and concerns to assess them.

THIS PAGE INTENTIONALLY LEFT BLANK

III. TECHNOLOGY CONSIDERATIONS

The aspect that gives the EDL its character—some argue a character flaw—is the technology embedded within the ID. Because the technology defines the EDL, an examination of the technology is required. Also necessary is a comparative analysis of the EDL's technology with other common ID technologies, which will help gauge whether the technology is appropriate and whether it offers a more secure solution to REAL ID complaint driver's licenses. Importantly, analysis will provide the backbone to the "necessary" technological changes. The focus will be on the technologies superimposed on or within the ID, particularly, the strengths and weaknesses critics have described as a security or privacy issue. Systems that extend beyond the ID such as readers will not be analyzed or will be briefly described.

A. A SHORT HISTORY OF RFID FOR BORDER CONTROL

The earliest use of RFID technology for access control is the electronic door lock opened by an RFID key card, which was patented by Charles Walton in 1973.[94] Practical use of RFID technology, however, has a rich history dating back to World War II, when the British used the technology to identify friend and foe aircraft.[95] Advancements in recent decades have reduced the size and cost of RFID technology and as such, have increased the number of purposes (supply chain management, tracking livestock, controlling building access) to include access control for the border.[96]

The first recorded use RFID technology for U.S. borders is the SENTRI card deployed in November of 1995, which came about as a result of Al Gore's "Vice President's National Partnership for Reinventing Government" initiative to streamline government.[97] The SENTRI program commenced in Otay Mesa, California, to vet low-

---

[94] Rieback, Melanie, Crispo, Bruno and Andrew Tanenbaum, "The Evolution of RFID Security," *Pervasive Computing* (January-March, 2006): 62-64.

[95] Mark Roberti, "The History of RFID Technology," RFID Journal, http://www.rfidjournal.com/article/print/1338 (accessed September, 19, 2012).

[96] Jeremy Landt, "The History of RFID," *IEEE Potentials* (October-November, 2005): 8-11.

[97] "Inspection of the Secure Electronic Network for Travelers' Rapid Inspection." USDOJ/OIG, http://www.justice.gov/oig/reports/INS/e0019/bckgnd.htm (accessed September 19, 2012).

risk border crossers for use of a dedicated lane and cursory check. A June 2000 evaluation of the program (before 9/11) indicated wait time in the SENTRI lane was lower than the general inspection lanes and there was greater confidence in security. The report did not ascertain, however, if the general inspection lanes wait times increased as a result of losing a lane(s) to SENTRI users.[98] The program, nevertheless, prompted other similar programs (NEXUS in June of 2002, FAST in December of 2002).[99]

The next evolution in RFID technology for border control was e-passports (see Figure 6). E-passports began as a result of collaboration between a United Kingdom software company, Digital Locksmith, and a Malaysian hardware company, Iris Corporation, at about the same time SENTRI was employed in the United States. Malaysia, as a result, was the first to deploy RFID in passports in 1998.[100] The same year, the New Technologies Working Group (NTWG) of the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD) began a study in support of the ICAO chartered under the U.N. to find a technical solution for electronic passports.[101]

Figure 6. Electronic Passport. From Electronics-Lab

98 "Inspection of the Secure Electronic Network for Travelers' Rapid Inspection." USDOJ/OIG, http://www.justice.gov/oig/reports/INS/e0019/results.htm (accessed September 19, 2012).

99 "CBP's Trusted Traveler Systems using RFID Technology Require Enhanced Security (Redacted)." Department of Homeland Security Office of Inspector General, http://www.oig.dhs.gov/assets/Mgmt/OIGr-06-36_May06.pdf (accessed September 20, 2012).

100 "ePassport." Digital Locksmiths, http://www.digitallocksmiths.com/ePassport.html (accessed September 19, 2012).

101 "Machine Readable Travel Documents, Part 1, Volume 2." International Civil Aviation Organization, http://hasbrouck.org/documents/ICAO9303-pt1-vol2.pdf (accessed September 19, 2012).

In the wake of 9/11, the U.N. adopted RFID-enabled passports in 2003 as the international standard based on the recommendations made by the NTWG of the TAG/MRTD. The RFID technical solution was premised on several factors; in particular, it had to be non-proprietary, available worldwide for global interoperability, useable in paper/cloth passports, have adequate memory capacity to hold a facial biometric and possibly more, and easy to fit into a reader. Nations were to remain responsible for maintaining and controlling databases while considering the use of other biometrics (iris scan, fingerprint) to augment the international standard facial biometric decided on (facial biometric was considered less invasive than other biometrics).[102]

As of August 2007, the U.S. requires all passports to be electronic.[103] Since 2007, thus, the use of RFID technology as a means of facilitating the verification of identity at U.S. borders has grown substantially. In fact, more than 99 percent of the inbound vehicle traffic at U.S. borders is verified via RFID technology and has contributed the DHS's 2011 reported success rate of 97-percent verification of travelers passing the U.S. northern borders.[104] Needless to say, the use of RFID technology for border control is now commonplace in the U.S and around the world and as such, unlikely to be usurped by another technology in the near future. Yet, may types of RFID technology exist and modifications or improvements to RFID have and continue to be made and as such, suggestions for improvement are available.

B. THE TECHNOLOGY ARGUMENT IN A NUTSHELL

According to the DHS, vicinity read (long-range) RFID-enabled EDLs offer several benefits. Foremost, this technology increases ID security. Expressly, it adds a level of credibility that the ID belongs to the individual that it has been issued to, which is a function of comparing the RFID's unique serial number and the non-rewritable TID

---

102 Ibid.

103 "The U.S. Electronic Passport Frequently Asked Questions." U.S. Department of State, http://travel.state.gov/passport/passport_2788.html (accessed September 19, 2012).

104 "Implementing 9/11 Commission Recommendations." U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/implementing-9-11-commission-report-progress-2011.pdf (accessed September 19, 2012).

number embedded on the tag with database information.[105] The long read range, arguably, also expedites border crossings by pre-positioning an individual's data before agent verification.[106]

Opponents of vicinity read EDLs point out fundamental flaws.[107] First, RFID is not an authorization alone; the ID still must be verified—handled—at the border and as such, the long-range RFID is unnecessary. Second, no law specifies the type of technology required on driver's licenses and as such, other technologies could be employed with greater emphasis on privacy. Third, not all border-crossing documents use a long-range RFID solution—for example, e-passports do not—diminishing the implied need for long-range RFID.[108]

C. THE RFID BASICS FOR IDENTITY DOCUMENTS

RFID technology is a contactless means of gathering data through the use of inductive coupling or backscatter radio waves—magnetic near field versus electric far field.[109] The use of radio waves, thus, allows data to be transmitted and received through solid materials. The system comprises three basic components: a transponder or tag with antenna for transmitting data; a reader (mobile or stationary); and the middleware or management system for translating, reading, or writing data to or from the tag through the reader for a specific purpose (see Figure 7).[110] Each component has features that affect functionality or capability. The most important is the tag embedded into the ID.

---

105 Manaher, *Privacy Impact Assessment for the use of Radio Frequency Identification (RFID) Technology for Border Crossings*, 23.

106 "The use of RFID for Human Identification: A DRAFT REPORT from DHS Emerging Applications and Technology Subcommittee." Homeland Security, http://seattletimes.nwsource.com/news/business/links/rfidprivacy.pdf (accessed May 9, 2012).

107 "Radio Frequency Identification (RFID) Systems."

108 "ACLU Says Enhanced Driver's Licenses are Insecure, Fail to Protect Personal Information." American Civil Liberties Union, http://www.aclu.org/technology-and-liberty/aclu-says-enhanced-driver's-licenses-are-insecure-fail-protect-personal-infor (accessed May 26, 2012).

109 Elisabeth Ilie-Zudor and others, *The RFID Technology and its Current Applications* (Department of Production Informatics, Management and Control, BME Hungary: The Modern Information Technology in the Innovation Processes of the Industrial Enterprises, 2006).

110 "The Basics of RFID Technology." RFID Journal, http://www.rfidjournal.com/article/articleview/1337/1/129/ (accessed September 20, 2012).

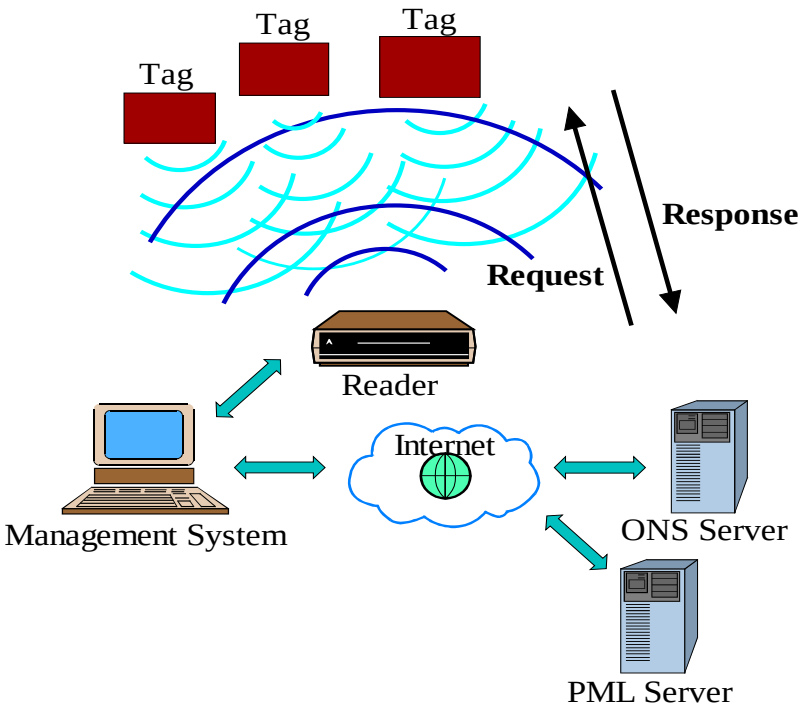

Figure 7. RFID System.[111]

Tags are classified as passive, active, or semi-passive and come in various shapes and sizes (Figure 8). Some are smaller than a grain of sand.[112] Passive tags, unlike active tags, contain no internal battery and depend on current from RFID readers for power.[113] Most passive tags store a few bytes of data, though prototypes are underway that can store as much as 500 kilobytes (KB).[114] Semi-passive tags have a battery but remain dormant until awakened by an RFID reader. Active tags are considered more reliable than

[111] Neeraj Chaudhry, Dale Thompson and Craig Thompson, "RFID Technical Tutorial and Threat Modeling Version 1.0," University of Arkansas, http://www.csce.uark.edu/~drt/publications/rfid-tutorial120608.pdf (accessed October 31, 2012). Figure represents a general RFID system. CBP and the DHS use a secure management system and a secure network.

[112] Tim Hornyak, "RFID Powder," *Scientific American* (February, 2008): 68.

[113] Roy Want, "An Introduction to RFID Technology," *Pervasive Computing* (January-March, 2006): 25.

[114] Steve Bush, "HP Passive RFID Chip Targets High Capacity Storage," Electronics Weekly, http://www.electronicsweekly.com/Articles/24/07/2006/39301/HP-passive-RFID-chip-targets-high-capacity-storage.htm (accessed August 27, 2012).

passive tags albeit more expensive and dependent on battery strength/life.[115] Basic active tags store 128 KB of data, though they are capable of more.[116]

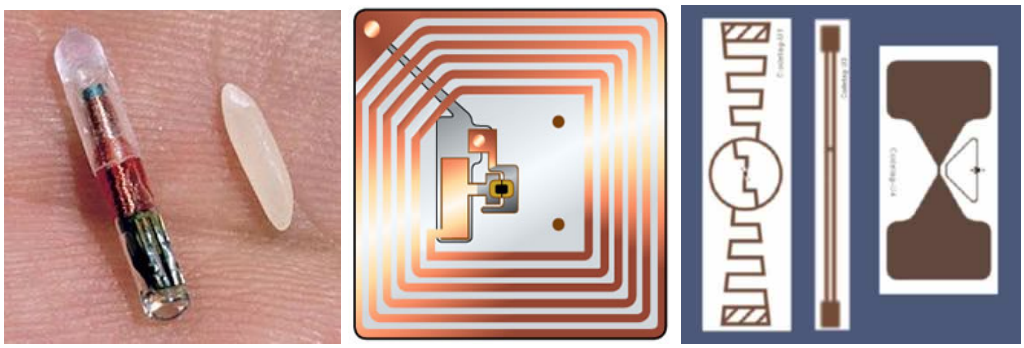

Figure 8. RFID Tag Examples. (From Wikipedia.com, RFIDvirus.org, and Made-in-China.com respectively.)

If the tag has read-write rather than read-only capability, data on the tag can be manipulated with or without the tag owner's consent. The tag does not alert when in contact with readers.[117] RFID-enabled ID systems do, however, use, at varying levels of complexity, the principle of mutual authentication (tag and reader must have matching key codes) and password protections to ensure the data on the tag cannot be accessed or manipulated.[118] If needed, RFID systems may also apply encryption.

Although the non-alert aspect is seemingly controversial for human IDs, the capability most often cited as a security or privacy issue is read range, expressly, the farther a signal transmits, the more likely it is to be intercepted with or without acknowledgement. A tag's read range depends on a number of factors, for example, type of tag, battery power, size of antenna, output of the reader, interference.[119] Generally

---

115 "The Basics of RFID Technology," 5.

116 Neil Jones, "RFID and the Difference between Passive and Active RFID Tags," Ezine Articles, http://ezinearticles.com/?RFID-and-the-Difference-Between-Passive-and-Active-RFID-Tags&id=3428256 (accessed August 27, 2012).

117 Nicole A. Ozer, "Rights "Chipped" Away: RFID and Identification Documents," *Stanford Technology Law Review* 1, no. 1 (2008), http://stlr.stanford.edu/2008/01/rights-chipped-away/.

118 Gerhard Hancke, "A Practical Relay Attack on ISO 14443 Proximity Cards," University of Cambridge, Computer Laboratory, http://www.rfidblog.org.uk/hancke-rfidrelay.pdf (accessed September 20, 2012).

119 Ozer, *Rights "Chipped" Away: RFID and Identification Documents*

speaking, passive tags have less read range than active tags. Despite the non-alert and read range security and privacy dilemma, read range and the ability to collect data simultaneous from multiple tags are the major advantages of the technology.[120]

Tags are made to respond to specific communication protocols from readers and operate on specific frequencies controlled by international standards organization (ISO) and International Electrotechnical Commission (EIC) for interoperability.[121] The four common passive tags used on U.S. ID applications are the ISO/EIC 14443 that operates at frequency of 13.56MHz, the ISO/EIC 15693 that also operates at frequency of 13.56MHz, the Electronic Product Code Class-1 Generation-1 (EPC-1) that operates at a ultra-high frequency (UHF) of 860MHz-960MHz and the Electronic Product Code Class-1 Gernatation-2 (EPC-2) that also operates at an UHF of 860MHz-960MHz (see Table 1).

1. ISO/EIC 14443

ISO 14443 is a passive-read, short-range contactless smart tag operable with readers at a nominal read range of six inches or less.[122] Tests have revealed, however, a potential read range of 30 feet.[123] Measures, such as faraday cage, can reduce read range to a few millimeters. As of today, the data transfer rate, that is, the communications speed, for these tags is 106 kilobytes per second (kbps)[124] with a storage capacity of up to 64KB.[125] In addition, these tags support a unique identifier (UID), 64-bit mutual authentication and a 32-bit password to protect data.[126] These tags apply encryption (e.g.,

---

120 Matt Metheny, *Radio Frequency Identification Technology (RFID): Securing the Homeland through Next Generation Identification Technology* (Washington D.C.: Lunarline, Inc., 2006).

121 Ibid.

122 Manaher, *Privacy Impact Assessment for the use of Radio Frequency Identification (RFID) Technology for Border Crossings*, 23.

123 Junko Yoshida, "Tests Reveal E-Passport Security Flaw," Electronic Engineering Times, http://www.eetimes.com/electronics-news/4049950/Tests-reveal-e-passport-security-flaw (accessed September 20, 2012).

124 "RFID and RF Memory Products Based on ISO 14443 and ISO 15693." STMicroelectronics, http://www.st.com/internet/com/SALES_AND_MARKETING_RESOURCES/MARKETING_COMMUNICATION/FLYER/flrfidrf.pdf (accessed September 20, 2012).

125 Nathalie Gosset, "What is ISO 14443?" eHow, http://www.ehow.com/about_6591701_iso-14443_.html (accessed September 20, 2012).

126 "Proximity Range - ISO/IEC 14443." Infineon, http://www.infineon.com/cms/en/product/chip-card-and-security-ics/contactless-memory-and-rfid-products/proximity-range-iso/iec-14443/channel.html?channel=db3a3043294a35580129643635c95140 (accessed September 20, 2012).

Data Encryption Standard [DES], 3-DES) as they are often used on valued ID applications with sensitive data/information, for example, U.S. e-passports or German national ID cards.

2. ISO/EIC 15693

ISO/EIC 15693 is a vicinity-read, long-range contactless smart tag, which is operable with readers at a read range of three feet. No tests were evidenced to determine the potential read range, yet it is likely greater than its ISO/EIC 14443 cousin. As of today, the data transfer rate for these tags is up to 53 kbps[127] and a storage capacity up to 8KB.[128] In addition, these tags support 64-bit UID, 64-bit mutual authentication and a 16-bit password to protect data,[129] and are capable of encryption. They are often used on less sensitive and short-duration ID applications, like ski resort IDs or patient IDs and thus, do not warrant the expense of encryption.[130]

3. EPC-1

EPC-1 is a vicinity-read, long-range contactless smart tag with a read range of 20 feet. No tests have yet determined the potential read range, though it is likely less than the upgraded EPC-2 tag (see below for potential range). As of today, the data transfer rate for these tags is up to 230 kbps, with a storage capacity of up to 96 bits.[131] These tags apply a weak mutual authentication method, a binary tree algorithm.[132] IDs that use this RFID solution—notably SENTRI, NEXUS, and FAST—only store a unique serial number for

---

127 "RFID and RF Memory Products Based on ISO 14443 and ISO 15693," 2.

128 "FRAM Embedded 13.56 Mhz RFID LSI." FIND, http://www.fujitsu.com/downloads/EDG/binary/pdf/find/30-3e/5.pdf (accessed September 20, 2012).

129 "TRF7960 Evaluation Module: ISO 15693 Host Commands." Texas Instruments, http://www.ti.com.cn/cn/lit/an/sloa141/sloa141.pdf (accessed September 20, 2012).

130 "Texas Instruments Expands Tag-it ISO/IEC 15693 RFID Product Line." PR Newswire, http://www.prnewswire.com/news-releases/texas-instruments-expands-tag-it-isoiec-15693-rfid-product-line-67541897.html (accessed September 20, 2012).

131 "Whitepaper: EPCglobal Class 1 Gen 2 RFID Specification." ALIEN, http://www.alientechnology.com/docs/AT_wp_EPCGlobal_WEB.pdf (accessed September 20, 2012).

132 Ibid.

identification and authentication purposes. Of note, most EPC-1 ID solutions are upgrading to EPC-2.[133]

4. EPC-2

EPC-2 is a vicinity-read, long-range contactless smart tag with a read range of 30 feet. Tests with commercially available equipment, however, revealed a read range of 217 feet with a potential read range of 565 feet, albeit at an expense of $2,500.[134] As of today, the data transfer rate for these tags is 640 kbps,[135] which is fast considering the data transfer rate for the most advanced cell phone systems are 220 kbps (average 14.4 kbps).[136] The max storage capacity for these tags is currently 64KB.[137] These tags support a more sophisticated method of mutual authentication (i.e., "Q" protocol: random number [0–15] algorithm) than EPC-1 tags with a 32-bit password to protect data.[138] IDs that use this RIFD solution store unique serial numbers for identification and authentication purposes (e.g., EDL, PASS card), thus, do not require the full capabilities of EPC-2 technology. The tag on the EDL, for example, has 256 bits of memory all of which has a specific purpose. Of note, EPC-2 is capable of 3-DES, yet it is an expensive option that defeats the intended purpose of the tag.[139]

---

133 Manaher, *Privacy Impact Assessment for the use of Radio Frequency Identification (RFID) Technology for Border Crossings*, 23.

134 Tim Greene, "Bad Guys could Read RFID Passports at 217 Feet, Maybe a Lot More," Network World, http://www.networkworld.com/news/2010/072910-black-hat-rfid-passports.html (accessed September 20, 2012).

135 "Whitepaper: EPCglobal Class 1 Gen 2 RFID Specification," 7-6.

136 Anton Shilov, "T-Mobile to Exclusively Sell Apple iPhone in Germany for T399," Xbit, http://www.xbitlabs.com/news/mobile/display/20070919164000.html (accessed October 21, 2012).

137 Claire Swedberg, "A Flurry of High-Memory Tags Take Flight," RFID Journal, http://www.rfidjournal.com/article/view/8295 (accessed September 20, 2012).

138 "Whitepaper: EPCglobal Class 1 Gen 2 RFID Specification," 7-6.

139 Mary Brown, "Security Challenges in RFID Implementations," *The ISSA Journal* (2006)

	ISO/EIC 14443	ISO/EIC 15693	EPC-1	EPC-2
Password	32-bit	16-bit	8-bit	32-bit
Mutual Auth.	64-bit	64-bit	Binary	Q-Protocol
Comm. Speed	106 kbps	53 kbps	230 kbps	640 kbps
Memory	64KB	8KB	96-bit	64KB
Intended Range	6 inches	3 feet	20 feet	30 feet
Encryption	Yes	Optional	No	No (Capable)

Table 2. Tag Comparison

D. TECHNOLOGY CONCERNS FOR THE RFID-ENABLED EDL

The major concern for EDLs with an EPC-2 tag, though complex, is the method of mutual authentication. Researchers, in fact, have suggested it is a naïve method of mutual authentication,[140] which allows any malicious reader conforming to EPC standards to communicate with the EDL's tag. Without encryption to scramble data, therefore, the EDL's serial numbers are susceptible to malicious readers. Applying encryption technology, however, would make an inexpensive tag more expensive.[141] Still, "it is not impossible today to get low cost, long range, high speed passive RFID tags with encryption and high security."[142]

Although the EDL's data is relatively secure from tampering with a 32-bit password, it does not apply encryption or other "lightweight" cryptology methods researchers have proposed to protect data from malicious readers that could be done without increasing the expense of the tag.[143] The ID, thus, is the weakest link, as the security offered by the system does not blanket the tag. The EPC tags do, however, have a read-only TID feature that may be used as an authentication tool. The TID helps to

---

140 Mikko Lehtonen and others, "Securing RFID Systems by Detecting Tag Cloning," ETH, https://edit.ethz.ch/im/people/mlehtonen/ETH_SS_Pervasive09.pdf (accessed September 20, 2012).

141 Ibid.

142 "Smart Border Alliance: RFID Feasibility Study Final Report." U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachD.pdf (accessed September 20, 2012).

143 Jemal Abawajay, "Enhancing RFID Tag Resistance Against Cloning Attack," *IEEE Computer Society* (2009): 18.

ensure the EDL is not fraudulent, yet it is not a cryptographic countermeasure to protect RFID serial numbers from malicious readers.[144]

Because malicious readers can establish communication and read the RFID serial numbers on EDLs, the key concerns are cloning (creating a duplicate tag/ID), skimming (covertly copying or reading the unique RFID serial number), tracking (identifying when and where a tag is located based on the location of a reader), and profiling (discriminating based on a demographic).[145] Each of the categories has specific threats either to security, privacy, or both. Each are describe in depth below to include the concerns related to the EDL.

1. Cloning

Cloning is the ability to copy the RFID serial number from the EPC-2 tags on EDLs and use it to "spoof" systems—in this case, to undermine border security by tricking border control readers into accepting an illicitly duplicated ID. Cloning is a known weakness of RFID.[146] In a 2009 demonstration for example, a researcher driving around San Francisco demonstrated how easy it is to clone EPC-2 tags with $250 in off-the-shelf Motorola reading equipment.[147] In fact, EPC readers are readily available for purchase on the open market, including devices for cell phones and USB devices under $200 for laptops.[148] Of course, the EPC was intended to supplant barcode technology, which means it is readily read by design. To some extent, this readability is offset by "kill passwords" for EPC tags that, ironically, are for privacy or security.[149] EDL tags are, however, designed with such measures as specific mutual authentication key code

---

144 Katherine Albrecht, "RFID TAG - YOU'RE IT," *Scientific American* 299, no. 3 (September, 2008, 2008): 72.

145 Ozer, *Rights "Chipped" Away: RFID and Identification Documents*

146 Ibid.

147 Thomas Ricker, "Video: Hacker War Drives San Francisco Cloning RFID Passports," Engadget, http://www.engadget.com/2009/02/02/video-hacker-war-drives-san-francisco-cloning-rfid-passports/ (accessed September 20, 2012).

148 Claire Swedberg, "MTI Creates EPC Gen 2 USB Reader for Retailer Applications," RFID Journal, http://www.rfidjournal.com/article/view/7540/ (accessed August 27, 2012).

149 Mary O'Connor, "EPC Tags Subject to Phone Attacks," RFID Journal, http://www.rfidjournal.com/article/view/2167 (accessed October 21, 2012).

methods built in; thus, not just any off-the-self device will be able to read the serial numbers from EDLs.

The security countermeasure on EPC-2 tags is the TID serial number embedded on the tag, which was not evidenced on earlier tested EDLs, in which TIDs were generic.[150] The TID, however, is not an anti-cloning mechanism. The TID, in fact, could be cloned as easily as the RFID serial number.[151] Yet, the cloner would likely need to obtain a tag with a programmable TID to fully clone or counterfeit the EDL. Companies are not likely to sell tags with programmable TIDs—unless one considers a state sponsored actor. Tags are built in many nations to include China, Malaysia and Taiwan.[152] Still, the TIDs do make it difficult for hackers or terrorists to clone an EPC-2 tag to subvert border security.

Long-read range may, however, be a problem if both the serial number and TID can be cloned.[153] The RFID in the EDL, for example, could be disabled to allow another RFID system to broadcast the appropriate signals from within the appropriate read-range while presenting a fraudulent EDL. The weakness, therefore, will require other security countermeasures such as driver's license plate technology at the borders. Detecting cloned tags is, however, a possibility.[154]

E-passports, in comparison to EDLs, use cryptographic overlays rather than the TID feature to ensure the ID is authentic and to prevent cloning.[155] Between passive (digital signature of issuing nation) and active authentication (digital signature of passport), the cryptographic features provide confidence that the passport belongs to the individual presenting it. Combined, they are a formidable means of preventing fraudulent

---

150 Karl Koscher and others, "EPC RFID Tag Security Weaknesses and Defenses: Passport Cards, Enhanced Drivers Licenses, and Beyond," University of Washington, www.cs.washington.edu/homes/yoshi/papers/RFID/css280-koscher.pdf (accessed May 10, 2012).

151 Manfred Aigner and others, "White Paper: RFID Tag Security," Bridge, http://www.bridge-project.eu/data/File/BridgesecuritypaperDL_9.pdf (accessed September 20, 2012).

152 Ibid.

153 Ibid.

154 Lehtonen and others, *Securing RFID Systems by Detecting Tag Cloning*, 18-2.

155 "Comparing Security of E-Passport and Passport Card/Enhanced Driver's License." Center For Democracy & Technology, https://www.cdt.org/security/identity/20071231passcard.pdf (accessed September 20, 2012).

IDs. Importantly, the e-passport is a critical component of the security system (see Table 2).

E-Passport Security	Enhanced Driver's License Security
Short-range RFID technology	Long-range RFID technology
Designed for privacy & security	Designed for cheap cost, speed & range
Basic Access Controls to lock & unlock	
Non-Traceable Chip	
Passive Authentication	
Active Authentication	
Extended Access Control	
RFID shielding (continuous protection)	Protective sleeve (random protection)

Table 3. E-Passport Security vs. EDL Security

2. Skimming

Skimming is the unauthorized access or capture of the EDL's unique RFID serial number for illicit reasons.[156] The user's RFID serial number could, for example, facilitate identity theft if the unique serial number is tied to a database with other PII. The threat of skimming EPC-2 tags, like cloning, has been confirmed by researchers,[157] as is the use of unique identifiers, for example, Social Security numbers, to facilitate identity theft.[158]

Another concern associated with skimming is the ability to aggregate RFID serial numbers to understand individual predilections.[159] If tagged repeatedly at enough locations, for example, individualized EDLs serial numbers could reveal sexual preferences, religious affiliations, political affiliations, spending preferences, entertainment preferences, and other predilections. Although this prospect seems far-

---

[156] Ari Juels, David Molnar and David Wagner, "Security and Privacy Issues in E-Passports," The California State Library, http://www.library.ca.gov/crb/rfidap/docs/JuelsetalI-SecurityandPrivacyofE-Passports.pdf (accessed August 27, 2012).

[157] Alice Lipowicz, "New Federal ID Cards Easily Cloned, Study Says," Federal Computer, http://fcw.com/articles/2008/10/24/new-federal-id-cards-easily-cloned-study-says.aspx (accessed September 20, 2012).

[158] Kristin Finklea, "Identity Theft: Trends and Issues," Congressional Research Service, http://www.fas.org/sgp/crs/misc/R40599.pdf (accessed September 20, 2012).

[159] Ozer, *Rights "Chipped" Away: RFID and Identification Documents*

fetched, the motivations for doing so are evidenced today by such on-line businesses as Google or Facebook[160] and such retailers as Walmart or CVS[161] that seek to streamline business dynamics to customer preferences—and collect volumes of information on customers to do it.

The DHS's countermeasure for skimming is a protective sleeve (see Figure 8) and privacy awareness training.[162] As long as EDLs remain in the sleeve, the signal is negligible—less than ten inches. Crumpled sleeves do, however, affect the read range, making the EDL readable up to 20 inches.[163] The DHS is concerned about skimming, including REAL ID driver's licenses (with no RFID), and has encouraged states to address these issues through state statutes.[164]

Figure 9. Protective Sleeve. (From 3M.)

A complicating factor in using EPC-2 tags on EDLs and other EPC-2 IDs is their original purpose, to replace barcodes. Specifically, more incentives for developing or fabricating skimming technology exit as a result of the rich business environment that

160 "How Companies are 'Defining Your Worth' Online." NPR, http://www.npr.org/2012/02/22/147189154/how-companies-are-defining-your-worth-online (accessed August 27, 2012).

161 Thomas Davenport, Leandro Dalle Mule and John Lucker, "Know what Your Customers Want before they Do," Harvard Business Review, http://theinformationdj.com/wp-content/uploads/2012/02/know-what-your-customer-wants-before.pdf (accessed August 27, 2012).

162 Manaher, *Privacy Impact Assessment for the use of Radio Frequency Identification (RFID) Technology for Border Crossings*, 23.

163 Koscher and others, *EPC RFID Tag Security Weaknesses and Defenses: Passport Cards, Enhanced Drivers Licenses, and Beyond*, 10.

164 "Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes [73 FR 5271][FR 5-08]," 1.

exists around the tags. This same deficiency could, however, be a blessing in disguise. The business world is also concerned about others hacking EPC-2 technology for intelligence (for instance, a business seeking to better understand the competition) or sabotage (for example, spoofing orders to customers).[165] Thus, the technology used in EDLs should improve alongside the business world, although ID cards are in circulation longer than most commercial products with EPC-2 tags.

Another complicating factor in using EPC-2 tags on EDLs is the long read range combined with the multipurpose nature of a driver's license. Driver's licenses are used in multiple situations, to include but not limited to, verification of signature for credit card purchases, proof of identity during a traffic stop, proof of identity for some air travel, and proof of identity when conducting such business as financial transactions or real estate transactions. Thus, the EDL's long-range signal will be exposed more often than other IDs, not least because the EDL must come out of its protective sleeve more often. In contrast, other border control IDs can be left in the protective sleeve or placed on a shelf or in glove box until needed with less concern.

3. Tracking

Tracking is the ability to discern an EDL's RFID serial number by location.[166] Although the signal can be triangulated,[167] the ability to discern location based on the tags read range and reader location is most compelling.[168] A concern today, for example, is the tracking of employees in the workplace by employers.[169] Since EDLs are multipurpose and discernable beyond U.S. land borders – for example, Canada and Mexico – it stands to reason, then, that many entities will have the potential to track U.S. citizens. It goes without saying that foreign governments have an interest in U.S. interests and people.

---

165 Abawajay, *Enhancing RFID Tag Resistance Against Cloning Attack*, 18.

166 Juels, Molnar and Wagner, *Security and Privacy Issues in E-Passports*, 14.

167 Simon Holloway, "Real Time Location Systems are the New Buzz in RFID," The Register, http://www.theregister.co.uk/2007/08/21/aeroscout_location_systems/ (accessed September 18, 2012).

168 Ilie-Zudor and others, *The RFID Technology and its Current Applications*, 31.

169 Marisa Pagnattaro, "Getting Under Your Skin-Literally: RFID in the Employment Context," *Journal of Law, Technology & Policy* 2 (2008): 237.

Some contend that the U.S. government could use ability to skim and collect serial numbers simultaneously to track masses of people.[170] The fear of such "Big Brother" tracking is referred to as a chilling effect.[171] Specifically, it may cause citizens refrain from such political activities as rallies or protests, because they believe that if tagged the government may retaliate.

Another fear associated with tracking is the potential for blackmail. Blackmail involves coercing an individual by threatening to expose a secret—a sexual preference, an affair—which often involves hush money.[172] Blackmail could also include other "payments," such as prevailing on a Congressman to vote against his beliefs or his constituency's interests to keep his dirty laundry well hidden.

4. Profiling

With the ability to skim and discern EDL RFID serial numbers, the ultimate fear is profiling or discriminating. The example studies site is IBM's "Margaret Program," in which RFID-enabled IDs gave bank employees in Britain early warning of affluent customers entering their facility.[173] Thus, the rich were receiving better service than the less affluent. Theoretically, therefore, RFID-enabled IDs could facilitate many other types of discrimination based on other demographics—age, gender, ethnicity, and political affiliation—especially if on a common ID.

E. A TECHNOLOGY COMPARISON OF IDENTITY DOCUMENTS

The EDL includes the technological features of a regular driver's license, which commonly includes 2D barcode and/or magnetic stripe (see Figure 9). Driver's license technologies are approved and standardized by the AAMVA and are designed to store and encode data, as well as to facilitate state database queries and to help prevent

---

170 Jay Stanley and Barry Steinhardt, "Even Bigger, Even Weaker: The Emerging Surveillance Society: Where are we Now?" American Civil Liberties Union, https://www.aclu.org/files/pdfs/privacy/bigger_weaker.pdf (accessed August 27, 2012).

171 Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review* 154, no. 3 (January, 2006c): 495.

172 Solove, *A Taxonomy of Privacy*, 485.

173 Jennifer Smith, "You can Run, but You Can't Hide: Protecting Privacy from Radio Frequency Identification Technology," *North Carolina Journal of Law & Technology* 8, no. 2 (Spring, 2007): 249.

counterfeiting and fraud.[174] With such measures already in place, one might raise the question of whether RFID technology is even necessary.

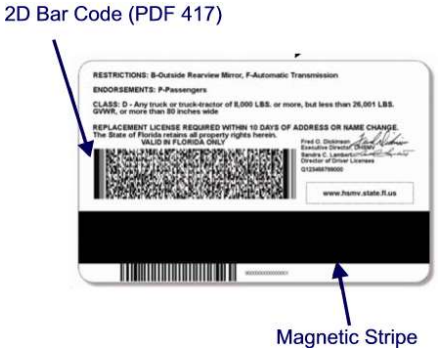

Figure 10. Driver's License Technologies. (From TOKENWORKS.)

Since all ID technologies have substantial memory capacity to hold a unique identifier, the fundamental question is whether other machine-readable technologies have similar or superior security features with the ability to authenticate, that is, the function the TID provides. Alternative technologies abound, but the most common are the barcode, the magnetic stripe, and the Smart Card. How does each stack up against RFID?

1. Barcode

Barcode technology is the most popular method for encoding personal information on a driver's license. The technology is capable of storing up to 32KB—China has proprietary rights on this design—but only 1.5KB (data matrix design) or 1KB (PDF 417) under U.S. property rights. Title 6 CFR 37.19 recognizes ISO/IEC 15438:2006(E) for REAL ID driver's licenses, which is PDF 417 barcode design.[175] Immediately, therefore, RFID is superior in terms of potential storage capacity.

The primary purpose of barcodes is to encode the information that is already on the driver's license for quick mechanical scanning, as well as to provide quick access to state databases from authorized terminals if necessary. Although a reader is required to

---

174 "Personal Identification - AAMVA North American Standard - DL/ID Card Design."

175 "37.19 Machine Readable Technology on Driver's License Or Identification Card." U.S. Citizenship and Immigration Services, http://www.uscis.gov/ilink/docView/6CFR/HTML/6CFR/0-0-0-1/0-0-0-4972/0-0-0-5292.html (accessed September 20, 2012).

discern information stored on a barcode, the hardware and software systems to do so can be found on the Internet.[176] Reading speed is approximately four seconds.[177] Compared to the much faster RFID, thus, the barcode technology has less storage capacity, less security potential, and less privacy potential. RFID, thus, is superior.

2. Magnetic Stripe

Magnetic stripe is a popular encoding technology for driver's licenses, yet Title 6 CFR 37.19 does not recognize it; it is optional for state purposes. Magnetic stripe typically has three tracks that hold 79 bits, 40 bits, and 107 bits respectively.[178] The technology as applied to driver's licenses, like barcodes, is designed for interoperability and ease of use and as such, can be accessed easily. Magnetic stripe technology, however, is capable of 3-DES and authentication that is approved by the federal government to secure sensitive data.[179]

Despite the security potential of the technology, the magnetic stripe is susceptible to wear and tear and can be copied easily, for instance, to create a duplicate ID. PIN codes are a countermeasure, though because PIN codes take time to enter, commerce would be severely impacted if instituted for border security or other commerce-related activities (e.g., scan barcode, retrieve PIN, enter PIN, and thereby authenticate ID). Magnetic stripe, thus, does not rise to the capabilities offered by RFID solutions.

3. Smart Card - Contact Technology

Smart Card (see Figure 10) is not a technology currently used on U.S. driver's licenses; however, it is a technology that could be applied to IDs, for example, military ID cards, and thus, can be applied to driver's licenses. Smart Cards are embedded

---

176 Dave Caldwell, "A Look at Your License," Minot Daily News, http://www.minotdailynews.com/page/content.detail/id/550887.html (accessed September 20, 2012).

177 Klaus Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, trans. Rachel Waddington, Second ed. (New Jersey: Wiley, 2006), 427-8.

178 "How does a Magnetic Stripe on the Back of a Credit Card Work?" howstuffworks, http://money.howstuffworks.com/personal-finance/debt-management/magnetic-stripe-credit-card1.htm (accessed September 20, 2012).

179 "FIPS PUB 46-3; Data Encryption Standards." U.S. Department of Commerce, National Institute of Standards and Technology, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf (accessed September 20, 2012).

microprocessors that are currently capable of containing over 200KB of electrically erasable and programmable read only memory (EEPROM), over 16KB of random access memory (RAM), and over 380KB of random operating memory (ROM).[180] Like magnetic stripe and RFID, the technology can support 3-DES and authentication.

There are three major drawbacks for this technology in comparison to RFID. Specifically, it is slightly more expensive, slower than RFID, more susceptible to wear and tear, and international interoperability standards have yet to be established.[181] Nevertheless, the technology could be employed that would alleviate the privacy concerns associated with RFID. All factors considered, however, RFID technology is superior.

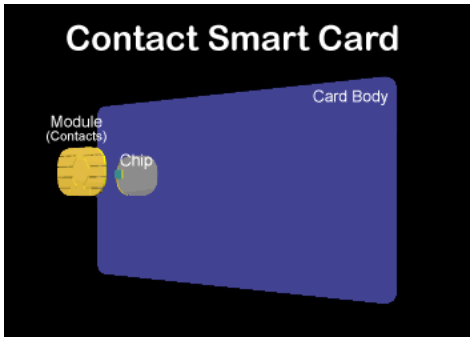

Figure 11. Contact Smart Card. (From The University of Chicago Department of Computer Science.)

F. OTHER TECHNOLOGY CONSIDERATIONS

An important consideration that should be made when assessing technologies on a common ID like the driver's license is expandability, that is, memory capacity. The ICAO, for example, established RFID technology as the international norm on e-passports for the purpose of storing the biometric facial image capture—quality images

180 "Samsung Announces High Performance Smart Card IC with 90-Nonometer Technology." Samsung, http://www.samsung.com/global/business/semiconductor/news-events/press-releases/detail?cateSearchParam=N011&searchTextParam=&startYyyyParam=&startMmParam=&endYyyyParam=&endMmParam=&newsId=4046&page=&searchType=C&rdoPeriod=A (accessed September, 20, 2012).

181 Kim Won and He-Joon Kim, "Smart Cards: Status, Issues, and US Adoption," *Journal of Object Technology* 3, no. 5 (May-June, 2004): 25-30.

take as much as 4KB of memory—and PII, for example, name, citizenship.[182] As of late, neither REAL ID nor WHTI requires biometrics to be stored electronically on the driver's license, though future security requirements may demand it.

Another technological consideration for a common ID like the driver's license is duration of use. Specifically, driver's licenses are typically in service for five or more years. REAL ID authorizes up to eight years, which is three years beyond the authorized life of other border IDs. As such, the technology employed on or within the driver's license may become increasingly susceptible to fraudulent activity as the technology ages. The RFID currently employed on EDLs, for example, could become further susceptible to cloning, skimming, and tracking as the technologies to do these activities become more sophisticated than the technology embedded in the driver's license. Thus, the need to ensure the technology is solid or flexible enough to support future changes if necessary.

Lastly, it is important to recall that the value of the driver's license is much greater than most other IDs in terms of the access it gives the bearer to myriad daily activities beyond plying the nation's roadways. As such, the technology should be sophisticated enough to resist counterfeiting. The e-passport, for example, is ostensibly secured by sophisticated technology because of the PII stored on it. Yet because PII is in plain view on the passport, it is largely a function of security and/or preventing those who would seek to counterfeit it. The same holds true for a driver's license, as they too are desirable IDs to obtain and perhaps greater as a result of branding them "enhanced."

G. THE TAKE-AWAY AND SOLUTION

Based on the bits and bytes of this chapter, several technological aspects of the current EDL are evident. First, RFID is the favored technology for good reason, as it is a reliable and inexpensive technology with a wealth of capabilities. Second, RFID offers optional degrees of security and read-range. Third, EPC-2 technology is susceptible to cloning, profiling, skimming, and tracking by malicious readers without encryption. Fourth, a state driver's license is more susceptible to cloning, profiling, skimming and

182 "Machine Readable Travel Documents, Part 1, Volume 2," 128.

tracking as a result of applying a long read-range technology to a common and multiuse state driver's license. Fifth, the use of EPC-2 technology on an inherently valuable ID in circulation for potentially eight years is precarious. The solution to these issues: adopt a short-range encrypted RFID and/or Smart Card solution with some additional capacity to support future changes if necessary.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. PRIVACY CONSIDERATIONS

The aspect of the EDL that has received the most attention is the impact to individual privacy. Much of the literature consists of anecdotes or unempirical presumptions from EDL critics. Thus, an examination of privacy is needed to fill the gap in the literature. More useful would be a comparative analysis of the EDL's current technology with an improved encrypted short-range RFID or Smart Card solution, expressly, it will help gauge if the updated technology offers the solution to privacy concerns. Importantly, the analysis will reinforce the need for a new technical solution not only for the security reasons identified in the previous chapter, but also for privacy reasons.

A. THE PRIVACY AND NATIONAL SECURITY DEBATE

The DHS's approval of EDLs continues to receive criticism from privacy advocates and others warning of the dangers posed to individual privacy.[183] The focus is on the DHS's use of vicinity-read RFID, which detractors write off as unsecure, unnecessary, and uncontrollable.[184] Yet, the matter runs deeper. Some, for example, assert the technology may be a "sheep in wolf's clothing."[185] The inference is that the technology could be used for the Orwellian purpose of tracking for government or corporate desires associated with power, control, or greed. Further implied is that psychological mechanisms—social proof, liking, authority, commitment and consistency[186]—and other "Pavlovian" mechanisms as the media touting the benefits and convenience are purposefully designed to erode society's expectation of privacy to facilitate the process.[187]

---

183 "ACLU Says Enhanced Driver's Licenses are Insecure, Fail to Protect Personal Information," 2.

184 Albrecht, *RFID TAG - YOU'RE IT*, 72.

185 Katherine Albrecht and Liz Mcintyre, *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID* (Nashville, Tennessee: Nelson Communications, Inc., 2005), 273.

186 Robert B. Cialdini, *Influence: The Psychology of Persuasion*, EPub ed.HarperCollins, 2009).

187 Albrecht and Mcintyre, *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID*, 273.

For the EDL, thus, the heart of the matter concerns power. Anytime the U.S. government expands NIDS such as the EDL or other ID systems, it further diminishes the privacy and autonomy of its citizens and thereby shifts power away from its citizens.[188] The EDL, to include REAL ID, does expand NIDS. Specifically, U.S. citizens register, that is, share PII for an individualized government folder stored in a database, which then allows for additional information derived from the RFID or facial biometric surveillance systems to be added to that or another electronic folder—for example, border crossing location, time, date. There follows the subsequent ability to share or analyze this data to help "connect the dots."[189] The multi-purpose nature of a driver's license, combined with the capabilities of long-range RFID adds to the "unknown" element.

Fundamentally, the more information that is gathered and the more individualized folders the U.S. government may access and analyze, the less privacy and autonomy citizens have.[190] Expressly, citizens become more and more "boxed-in" with less privacy or autonomy—in a society that honors these rights as much as possible. At the same time, however, there is a need for identification systems in a society or world in which evils like terrorism and crime exist, especially when society has an expectation that government will provide some level of security against these threats. Likewise, healthy societies require some level of compliance, participation, and legitimacy that is often referred to as social control.[191]

Because identification, security, and social control are necessary, a balance must be struck between civil liberties and these other goals that are agreeable to society as a whole. The government has a significant responsibility in this process, which is to ensure that civil liberties are preserved as much as possible. Arguably, the government has done this. When Americans' favor of a national ID tipped over the 50-percent threshold after

---

188 Richard Sobel, "The Demeaning of Identity and Personhood in National Identification Systems," *Harvard Journal of Law & Technology* 15, no. 2 (Spring, 2002): 319.

189 Hamilton Bean, "Exploring the Relationship between Homeland Security Information Sharing & Local Emergency Preparedness," *Homeland Security Affairs* 5, no. 2 (May, 2009).

190 Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 319.

191 Joel Migdal, *Strong Societies and Weak States* (New Jersey: Princeton University Press, 1988), 296.

9/11,[192] for example, the government could have developed legislation for a national ID.[193] The federal government instead developed and enacted the IRTPA, while conceded some power under REAL ID, to tighten driver's license standards without imposing a unitary national ID requirement. Albeit not a perfect law, REAL ID is a much more agreeable solution than a national ID card that must be carried on person at all times—particularly with more than a decade of relative domestic tranquility since the 9/11 attacks to temper the fervor for stricter national ID standards.

A key component of the civil liberties and national security debate is the concession of power. The public's power or trust in government is something that the government can draw on in times when national security is threatened. The lower the level of trust, the less likely the government is able to succeed.[194] Implicit is that a compromise exists.[195] Thus, the debate is often cast in the conventional terms of national security versus civil liberties, on the assumption that as support for civil liberties increases, support for order and security decreases, and vice-versa.[196] Yet, one also might argue that civil liberties and security are not necessarily at odds. National security, itself, fosters civil liberties by providing the context for the stability and prosperity in which personal freedoms can reach their highest levels.

Because security does provide the context for personal freedoms to reach their highest levels, a tension will persist that government must contend with. The latest U.S. poll, unlike directly after 9/11, for example, indicates that the protection of rights and freedoms is more important to Americans than security.[197] The Pew Research Center also indicates a 7-percent increase from 2004 and 2009 in public attitudes favoring the

---

192 Heather Kiefer, "Do Americans Want National ID Cards?" Gallop, http://www.gallop.com/poll/6364/americans-want-national-cards.aspx (accessed September 20, 2012).

193 Alison M. Smith, "National Identification Cards: Legal Issues," Congressional Research Service, http://assets.opencrs.com/rpts/RS21137_20030107.pdf (accessed September 20, 2012).

194 Darren Davis and Brian Silver, "Civil Liberties Vs. Security: Public Opinion in the Context of the Terrorist Attacks on America," *American Journal of Political Science* 48, no. 1 (January, 2004): 28.

195 Gerald Baliles and others, *Public Debate Resolution: In the War Against Terrorism, and with Advances in Technology, Americans Need to Lower their Expectations of Privacy* (University of Virginia: Miller Center of Public Affairs, 2007).

196 Davis and Silver, *Civil Liberties Vs. Security: Public Opinion in the Context of the Terrorist Attacks on America*, 28.

197 D. Himberger and others, "Civil Liberties and Security 10 Years After 9/11," *The Associated Press-NORC Center for Public Affairs Research*, September 2011.

protection of civil liberties.[198] Without a clear and present national security threat on the proverbial horizon, thus, citizens of a democracy naturally reset their preferences to reflect the innate distrust of a large, intrusive state apparatus, even if it calls itself "security." At some point, therefore, the government must abdicate power back to the public, as necessary, or risk a popular dissent.

Since security and civil liberties are not necessarily at odds, security systems or methods must be closely scrutinized whenever it is inferred that civil liberties are threatened. Given the RFID-enabled EDL privacy debate, thus, an opportunity exists to peel back the layers to determine if an unnecessary concession of power exists under the guise of security. Importantly, analysis will provide a greater understanding of the privacy issues and, if necessary, mitigate them. Striking the perfect balance between privacy and national security, however, is more of an art than a science as either end can be jumped on to pull against the other. Because the fundamental argument made by privacy advocates is that the long-range RFID of an EDL is a threat to the right to privacy, the right must be assessed to determine if greater protections are necessary to preserve privacy. The right to privacy, however, exists on two planes, specifically at the Constitutional level for state concerns and at the tort level for private entity concerns.

1. The Constitutional Right to Privacy vs. RFID

The right to privacy is not in the Constitution nor is it clearly spelled out in the Bill of Rights as, for example, the right to a fair trial or the freedom of assembly is. It has culminated, as a legal concept, in the last century as a right from such articles of the Bill of Rights as the First Amendment (privacy of beliefs), the Third Amendment (privacy of home), the Fourth Amendment (privacy of person and possessions), and more generally the Fifth, Ninth and Fourteenth Amendments.[199]

---

198 "U.S. seen as Less Important, China as More Powerful: Isolationist Sentiment Surges to Four-Decade High." Pew Research Center, http://www.people-press.org/2009/12/03/section-7-threat-of-terrorism-and-civil-liberties/ (accessed May 26, 2012).

199 "The Right of Privacy." University of Missouri Kansas City, http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html (accessed August 27, 2012).

Scholars cite Samuel D. Warren and Louis D. Brandeis as the first jurists to articulate the legal theory of privacy in an 1890 *Harvard Law Review* article.[200] Coining the phrase "the right to be let alone" by paraphrasing Thomas Cooley, [201] Warren and Brandeis argue laws should protect an individual from unwarranted invasions by the state.[202] Little has changed in this basic interpretation. The courts have generally agreed that American citizens are protected from unreasonable invasions of privacy by the state. The Supreme Court's landmark decision in *Roe v. Wade*,[203] which provides a woman's right to choose the abortion of her child during the first trimester, exemplifies the right to privacy particularly as it relates to Ninth and Fourteenth Amendment.[204]

The ambiguity about the right to privacy, however, has made it "a concept in disarray as it seems to be about everything, and therefore it appears to be about nothing."[205] The incursion of technology in the last few decades has only added to the disarray.[206] In fact, the dynamic nature of technology has generated debate as to whether the courts or legislatures are in the best position to protect privacy. Expressly, the "courts have a difficult time keeping pace with technological change, and statutory schemes can quickly become outdated."[207] Nonetheless, both have been integral to shaping the right alongside technological development.

In dealing with state invasions of privacy from technology, the Fourth Amendment is the bedrock of "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…"[208] The key word is unreasonable, as it implies an interpretation, in the last

---

200 Dorothy J. Glancy, "The Invention of the Right to Privacy," *Arizona Law Review* 21, no. 1 (1979): 1.

201 Ibid.

202 Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (December 15, 1890): 193.

203 *410 U.S. at 113*, 1973

204 "Expanding Civil Rights." PBS, http://www.pbs.org/wnet/supremecourt/rights/landmark_roe.html (accessed August 27, 2012).

205 Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review* 154, no. 3 (January, 2006b): 479.

206 Levy, *Towards a Brighter Fourth Amendment: Privacy and Technological Change*, 502.

207 Levy, *Towards a Brighter Fourth Amendment: Privacy and Technology Change*, 504.

208 U.S. Constitution. Amendment IV

instance by a court, may be necessary. In fact, several technological advancements used by the state to facilitate prosecution have necessitated the court's interpretation of the right to privacy. The problem, in large part, is due to technological advancements used beyond their intended purpose for surveillance, for example, tracking through various technologies.

In *Kyllo v. United States,* for example, the court found that law enforcement requires a warrant before using a thermal-imaging device to detect heat patterns emanating from a person's home.[209] Similarly, in *United States v. Karo* the court believed it necessary for law enforcement to obtain a warrant before using a beeper to monitor the movements of persons while in their home.[210] The threshold is much higher outside of home. In *United States v. Knotts,* for example, court believed that the law enforcement's use of a beeper for tracking merely augmented their ability to do something that was visually observable in public.[211]

Implicit is that technology develops before the right to privacy is a concern and that the technology itself is not the automatic nemesis of privacy. In fact, most technologies—for example, beepers, RFID, global positioning systems (GPS)—are not developed for the purpose of invading privacy. It is only after technologies are developed that humans find ways to use them intentionally or unintentionally to undermine the right to privacy. Legislatures and courts, therefore, are typically plugging gaps in order to protect the right to privacy.

An important element for the right to privacy is the subjective interpretation, which is based on what society is prepared to recognize as reasonable. In *Katz v. United States,*[212] for example, the Supreme Court ruled warrantless wiretapping by the state violates the Fourth Amendment. The decision, however, was not strictly based on the Fourth Amendment. It also included a subjective element or what society was prepared to

---

209 *533 U.S. at 27*, 2001
210 *468 U.S. at 705*, 1984
211 *460 U.S. at 276*, 1983
212 *389 U.S. at 348*, 1967

accept as reasonable at that time.[213] It is implied, therefore, that as societies attitudes change, so too do court interpretations and legislative (re)actions.

It is generally understood that social attitudes toward privacy are continually flattened the by the influx of technology (often a function of convenience). The erosion of privacy is "a process through which a technology's gradual growth is followed by the perpetuation of an unforeseen invasive aspect that is shrugged off as the inevitable price of progress."[214] The more technologies interact with humans, therefore, the more erosion that can or will take place. Explicitly, the privacy threshold is continually increasing along side society, which is why some have argued for a "bright line" or clear parameters to protect privacy.[215]

2. Common Law Tort Right to Privacy vs. RFID

Although the United States Federal Trade Commission (FTC) permits RFID users to self-regulate,[216] individuals have a legal right to privacy so long as two elements are satisfied. First, the information used must be "highly offensive or objectionable to a reasonable man," and second, "the thing into which there is prying or intrusion is entitled to be, private."[217] Restatement protects individuals from "intentional intrusion, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns… if the intrusion would be highly offensive to a reasonable man."[218]

In tort, the motivations for RFID users to avoid violating privacy are monetary. Expressly, users can be sued or could lose business (or entirely) as a result of "backlash."[219] The class action lawsuit filed against Facebook for unlawfully monitoring

---

213 Levy, *Towards a Brighter Fourth Amendment: Privacy and Technology Change*, 507.

214 Ibid.

215 Ibid.

216 Serena G. Stein, "Where Will Consumers Find Privacy Protection from RFIDS? A Case for Federal Legislation," *Duke Law & Technology Review* 3 (2007). Author states, "With RFID technology third parties are able to secretly track individuals by "skimming" and "eavesdropping."

217 William J. Prosser, "Privacy," *California Law Review* 48, no. 3 (1960): 390.

218 Tom Bell, "Restatement (Second) of Torts: 652A-E (1997)," Tomwbell.com, http://www.tomwbell.com/NetLaw/Ch05/R2ndTorts.html (accessed August 27, 2012).

219 Levy, *Towards a Brighter Fourth Amendment: Privacy and Technology Change*, 502.

users even when they were not on-line is an example.[220] The "highly offensive" mark in court, however, could be a high hurdle for prosecutors. In *Dwyer v. American Express*, for example, the court did not hold the company liable for data-mining the plaintiff's spending patterns and selling it to merchants.[221]

With the ability to of RFID users to self-regulate and the challenges of tort law to redress privacy issues, there has been a call for federal legislation.[222] To date, no federal legislation has been considered. Many states, however, have enacted laws on many different issues related to RFID.[223] California, North Dakota, Oklahoma, and Wisconsin for example, prohibits requiring implantation of a RFID microchip. California, Nevada, and Washington prohibit unauthorized skimming. For EDLs, states have either adopted laws to accept, refuse, or place restrictions--so that only certain numbers can be issued, they must have encryption, no surveillance devices on highways, no compiling of data into a database, and no PII.[224]

B. CONTEXTUAL EVALUATION OF THE CURRENT EDL

When a new technology comes on-line, it must be defined in a specific context (tracking, profiling) and time (during a time of national emergency, peace) to evaluate privacy.[225] The privacy issue associated with a new airport X-ray device that can see through people's clothing, for example, is different than law enforcement using RFID-enabled ID for tracking. Even then, however, the contextual situation may be unreasonable but necessary, particularly when it is for the purpose of national security.

---

220 Gary Haber, "Angelos, Murphy Sue Facebook Over Privacy Rights," Baltimore Business Journal, http://www.bizjournals.com/baltimore/news/2012/02/22/baltimore-law-firms-sue-facebook-over.html (accessed August 22, 2010). Facebook argues that the lawsuit should be dropped as it fails to show how users were harmed, although the company did admit to the activity and said it was a mistake.

221 *Dwyer V. American Express Company*, 652 N.E. 2d, 1351 (Appellate Court of Illinois, First District, First Division 1995).

222 Stein, *Where Will Consumers Find Privacy Protection from RFIDS? A Case for Federal Legislation*

223 "State Statutes Relating to Radio Frequency Identification (RFID) and Privacy"

224 Ibid.

225 Solove, *A Taxonomy of Privacy*, 485.

Thus, the quote "the inevitable price of progress"[226] should be expanded to include "the inevitable price of progress or national security."

Because the EDL is used in multiple contexts, it is necessary to evaluate both the state (Constitutional) and private (tort) concerns. Although privacy concerns could be explicit, such as tracking inside or outside of the home, the general contextual concern will suffice. Specifically, the laws associated with privacy are applicable in all contexts—both in and outside the home—and it is only the interpretation or weight of the privacy invasion that is of significance.

1. State Concerns

The major common-law concern about the long-range RFID-enabled EDL is the ability of the state to track U.S. citizens without consent or a warrant. Given that RFID can be triangulated or narrowed down to a read range,[227] tracking is well possible—and represents a privacy concern.

The concern about the state tracking U.S. citizens without consent or a warrant assumes EDLs will be as effective or more effective than other means of electronic tracking. Beepers—cell phone technology—and GPS offer a much more effective means of tracking.[228] To assume, thus, that the state would prefer to track EDLs is dubious. After all, EDLs transmit at best 217 feet when exposed.[229] They do, however, provide the potential to track the card in perpetuity; once the state-issued EDL is voluntarily bought, ownership is transferred to the individual. In fact, the August 14, 2012 federal court ruling in *U.S v. Skinner* allowing law enforcement to track cell phones without a warrant based on their "inherent external locatability" could also be applied to EDLs.[230] The protective sleeve, however, would likely require the state to generate reasons for the EDL to be exposed and as such, it is likely more trouble than it's worth.

---

226 Levy, *Towards a Brighter Fourth Amendment: Privacy and Technology Change*, 506.

227 Holloway, *Real Time Location Systems are the New Buzz in RFID*

228 Tarik Jallad, "Old Answers to New Questions: GPS Surveillance and the Unwarranted Need for Warrants," *North Carolina Journal of Law & Technology* 11, no. 2 (Spring, 2010): 351.

229 Greene, *Bad Guys could Read RFID Passports at 217 Feet, Maybe a Lot More*

230 Michael Hoven, "United States V. Skinner: Sixth Circuit Approves Warrantless Tracking of Cell Phone Location," JOLT Digest, http://jolt.law.harvard.edu/digest/telecommunications/united-states-v-skinner (accessed October 6, 2012).

Scholars have noted that law enforcement has a knack for keeping up with new tracking technologies, which "invigorate in-house solutions that are kept secret."[231] Thus, it is unknown whether a technology will be developed to make RFID-enabled EDLs a viable tracking alternative. Either way, legal standards (*Kyllo v. United States*, *United States v. Karo*) and laws (the Omnibus Crime Control and Safe Streets Act of 1968, the Electronic Communications Protection Act of 1986) provide legal guidance and/or a recourse to abuses if the state uses RFID emitted from EDLs for the purpose of tracking albeit base on societies eroding expectation of privacy at that time.

Beyond individual tracking is the ability of the state to use RFID-enabled EDLs to facilitate mass tracking. While this eventuality is plausible, granted that RFID can be tracked at multiple locations, given the amount of digital data humans produce, this proposition, too, is doubtful. It is far easier and more advantageous to collect information or data from other systems, for example banking records, telephone records, Internet blogs, for all of which legal protocols exist, albeit stressed by new challenges.[232] Moreover, EDLs are not, as of late, mandatory or pervasive. Admittedly, however, EDLs are a mechanism for mass validation for the purpose of border control that is closely related to mass tracking. Thus, there remains the notion that EDLs could be used for this purpose.

2. Tort Concerns

There are three major tort-related concerns for the RFID-enabled EDL. The first is the ability of the RFID users to acquire the EDLs RFID number for the purpose of identity theft or understanding individual predilections. Given EDLs use an unencrypted EPC tag that emits a unique serial number tied to a database, this is a plausible contextual situation. The second is the ability of RFID users to conduct tracking. The third is the ability to profile, which is also possible with a unique RFID serial number.

The concern that the EDLs unique number, similar to the Social Security Number, will facilitate identity theft assumes RFID numbers will become commonplace and, thus,

---

231 Levy, *Towards a Brighter Fourth Amendment: Privacy and Technological Change*, 502.

232 Fred Cate, "Government Data Mining: The Need for a Legal Framework," *Harvard Civil Rights-Civil Liberties Law Review* 43 (2008): 435.

used in multiple systems. Because RFID numbers are unlikely to propagate beyond secure systems,[233] the notion that it will become as pervasive as SSNs is dubious; serial numbers will also change when new driver's license is issued. Section 18 USC 2721 does, however, have 14 permissible reasons for the PII to be disclosed from vehicle databases[234] that, arguably, have degrees of trustworthiness. Either way, it is a potential threat and one that has federal protections under The Driver Privacy Protection Act of 1994 and The Federal Identity Theft and Assumption Deterrence Act of 1998.[235] Thus, a legal recourse for abuse exists should the RFID number facilitate this activity. The building of profiles from serial numbers to understand individual predilections, however, is a concern as the legal recourse is suspect. [236]

The concern that EDLs will facilitate tracking by private entities does not hold much water as long as EDLs do not become pervasive. Private entities are more likely to tag and track products than risk a potential privacy invasion of tracking EDLs, which could destroy their business. Business and individuals who deal with people, however, could be of some concern--for example, a private investigator or an insurance company. As noted earlier, there are no federally enforceable RFID laws to control the tracking actions of businesses and private individuals.[237] The DHS has, however, encouraged states to deal with this potential issue and some have done so.

The final concern that EDLs facilitate profiling has foundation, yet it is unlikely to take off as a result of a covert undertaking. Expressly, EDLs are not yet common or mandatory and as such, they would be of little value as a discriminator. It is far more likely that users will facilitate this activity if does occur. For example, users could allow entities like banks, clubs, or businesses to record their RFID number for the purpose of

---

[233] Manaher, *Privacy Impact Assessment for the use of Radio Frequency Identification (RFID) Technology for Border Crossings*, 23.

[234] "18 USC 2721 - Prohibition on Release and use of Certain Personal Information from State Motor Vehicle Records." Cornell University Law School, http://www.law.cornell.edu/uscode/text/18/2721 (accessed September 20, 2012).

[235] *Identity Theft and Assumption Deterrence Act of 1998,* Public Law 4151, (1998): 105.

[236] Stein, *Where Will Consumers Find Privacy Protection from RFIDS? A Case for Federal Legislation*

[237] Ibid.

receiving perks—better service or establishing credit. The point is that it is less of a privacy issue and more of an ethical issue if it does occur.

C. DOES THE IMPROVED EDL ADDRESS PRIVACY CONCERNS?

Although some of the privacy concerns of the EDL with its current technology are debatable, some are not. The question, therefore, is whether or not a short-range encrypted and/or Smart Card technology offers a better solution for the EDL. There are two levels that must be assessed. The first is state-level concerns, expressly; it is only through state support that an improved driver's license will be feasible. The second, and no less important, is the individual privacy concerns. Although individual privacy concerns could be separated into state and tort concerns, the overlap in similarities makes it unnecessary.

1. State Concerns

As noted, some states have either denied or placed legal restrictions on EDL to include: only certain numbers can be issued; must have encryption; no surveillance devices on highways; no compiling of data into a database; and no PII on EDL.[238] Each, therefore, must be assessed with the proposed technological changes with the exception of the need for encryption as it is applied to the solution. The question is whether or not the remaining privacy concerns are addressed with an encrypted short-range or Smart Card EDL.

Beginning with the notion that only a certain number of EDL's can be issued; this ostensibly is a need to lessen the erosion of privacy or to ensure the EDL does not become pervasive to encourage privacy invasions or a national ID. Since an encrypted short-range or Smart Card EDL offers more security and privacy than even REAL ID compliant driver's licenses, the state concern is addressed. Further, the EDL could remain a state function that is audited and as such, the national ID not amplified beyond REAL ID compliant driver's licenses. The new solution(s), thus, addresses state concerns.

---

238 "State Statutes Relating to Radio Frequency Identification (RFID) and Privacy"

The "no surveillance devices on highways" notion is a consequence of the long-range RFID currently used on EDLs. The belief is that long-range RFID will facilitate surveillance or become an overt or covert E-Z Pass-like system to track U.S. citizens on highways.[239] The encrypted short-range or Smart Card solution nullifies the concern. The solution also addresses the "compiling of data into a database" as it too is a consequence of long-range RFID, for example, a person or entity clandestinely skimming RFID numbers. Thus, the encrypted short-range RFID and/or Smart Card solution addresses both state concerns.

The final state concern of "no PII on the EDL" is a little tricky. The DHS has indicated that privacy risks are mitigated because no PII is stored on the RFID tag.[240] The definition of PII by the U.S. Department of Commerce, however, suggests that the RFID's unique serial numbers are in fact PII because "it can distinguish an individual, trace an individual, and is linked to information about an individual."[241] Nonetheless, the serial numbers are no different than the exposed driver's license number and, thus, the new solution(s) does address the state concern, not to mention it is more secure than an exposed driver's license number.

2. Individual Concerns

Individual concerns of an unencrypted long-range RFID-enabled EDL can be framed under the following potential issues: tracking; identity theft; skimming serial numbers to understand individual predilections; and profiling. The question is whether or not an encrypted short-range or Smart Card technical solution will address each of these concerns.

The first concern of tracking is, in large part, a function of the EDL's long-range RFID. Since the proposed short-range RFID or Smart Card solution brings the signal to

---

239 "Title XX Transportation: Chapter 236 Highway Regulation, Protection and Control Regulations: Highway Video Surveillance." New Hampshire General Court, http://www.gencourt.state.nh.us/rsa/html/XX/236/236-130.htm (Accessed September 20, 2012).

240 Manaher, *Privacy Impact Assessment for the use of Radio Frequency Identification (RFID) Technology for Border Crossings*, 23.

241 Erika McCallister, Tim Grance and Karen Scarfone, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," *NIST, U.S. Department of Commerce* 800-122 (April, 2012): 2-1.

less than what can be visually observed, the notion of tracking is absolved. The short-range RFID solution does, even with encryption, have a latent ability to track that gives slightly more credence to the Smart Card solution. An RFID on/off switch, however, could be a solution to entertain solely the RFID technical solution and may support a slightly greater read-range.

The second concern of identity theft is a consequence of the EDL's unencrypted long-range RFID and as such, the new solution addresses this concern. Encrypted EDLs, in fact, close the loop to ensure all systems securely protect PII. Some of the PII that is visually observable on the EDL could actually be supported by the technology to further reduce the likelihood of identity theft. Importantly, the new solution severely reduces the ability to counterfeit, as serial numbers are secure and controlled by states.

The third and fourth concerns of skimming and profiling are a function of the unencrypted signal and long-range RFID. Since the proposed solution is encrypted and short range and/or Smart Card, both of these concerns are nullified. Thus, an encrypted short-range RFID and/or Smart Card solution address individual privacy concerns.

V. ASSESSING THE EDL

This chapter reinforces the need for an encrypted short-range RFID or Smart Card technological solution to support the voluntary EDL. It also reinforces the notion that the new solution(s) should be adopted nationwide to reduce the growing epidemic of counterfeit drivers licenses. It also demonstrates that the EDL, with the appropriate technology, offers more capabilities than REAL ID compliant driver's license and supports the notion that the EDL, with the appropriate technology, is less invasive on state and individual rights and could liberate many, if not all, of the IDs in support of the WHTI to reduce several NIDS.

A. POLITICAL ASSESSMENT

An encrypted short-range RFID and/or Smart Card EDL has the potential to be less invasive on state and individual rights beyond the ability to protect Fourth Amendment privacy established in Chapter IV. What has yet to be addressed is how. The subsections below will answer this question for the concerns identified in Chapter II, which consist of the following: Tenth Amendment concerns; First Amendment concerns and biometrics; restrictions on commercial air travel; national ID concerns; and privacy risks at the system level.

1. Tenth Amendment Concerns

Any federal mandate that imposes requirements on the states, particularly those that have been assigned to the state by the Constitution under the Tenth Amendment,[242] will be met with resistance, as the IRTPA and REAL ID revealed. Since the driver's license and identification card process is a state function, the federal government must respect state autonomy when developing legislation and the Executive must exercise discretion during interpretation of law. *Printz vs. United States,*[243] for example, confirms the federal government cannot impose a regulatory program, even if temporary, that is

---

[242] "About the Tenth Amendment." Tenth Amendment Center, http://tenthamendmentcenter.com/about/about-the-tenth-amendment/ (accessed September 20, 2012).

[243] *538 U.S. at 1036*, 2003

granted to a State. Since REAL ID is not compulsory, the Tenth Amendment is not violated and in a greater sense, the federal government is seeking support to bolster national security without resorting to a unitary national ID.

The fundamental question then is: how does an encrypted short-range RFID and/or Smart Card EDL better support the Tenth Amendment? The answer resides in the fact that EDL authentication can take place through state systems. Importantly, the EDL is currently and would remain a state and *not* a federal ID. States also control the designs of EDLs. Centralized authority over personal identity at the federal level, thus, is unnecessary. As a win-win, the federal government retains the ability to authenticate identity over secure systems "controlled and audited" by states.

If the EDL were to be adopted nationwide, it could alleviate the necessity of other, if not all, IDs in support of the WHTI to more emphasize state level ID systems. Privileges, such as speed lanes or commercial lanes, could be signified, if necessary, by other means. Removing WHITI IDs, in fact, will increase authentication checks of the EDL, and subsequently further reduce the likelihood of counterfeiting. Hence, an encrypted short-range RFID and/or Smart Card ID is less of an impact on the Tenth Amendment; could reduce Fourth Amendment privacy concerns of WHTI IDs; decreases the likelihood of counterfeits, and subsequently identity theft; increases national security; and has the potential to provide the freedom to traverse borders with a driver's license once known before 9/11.

2. First Amendment Concerns and Biometrics

The core necessity for a biometric is to "authenticate" identity."[244] With an "authenticable" EDL used by U.S. citizens, thus, the requisite is minimized. Importantly, it would not be necessary to mandate one particular biometric for U.S. citizens issued an EDL. States, in fact, should not, as in *New York vs. United States*,[245] be afforded minimal options by the federal government. Fingerprints, DNA, hand, optic scans, voice, and

---

[244] Michael Zimmerman, "Biometrics and User Authentication," SANS Institute, http://www.sans.org/reading_room/whitepapers/authentication/biometrics-user-authentication_122 (accessed October 21, 2012).

[245] *505 U.S. at 144*, 1992

signature, for example, are available biometrics that are as or more reliable.[246] With options, therefore, U.S. citizens who do not want their photo taken for religious reasons could be afforded an alternative. Moreover, it would relieve some of the fear that the government is "tracking" U.S. citizens with video surveillance systems. Thus, an encrypted short-range RFID and/or Smart Card ID solution has the potential to offer greater First Amendment protections. Moreover, both solutions reduce the "chilling effect" of long-range RFID.

3. Restrictions on Air Travel

The recent adoption of Global Entry cards to support air travel indicates U.S. citizens issued an EDL could be afforded the same benefits. U.S. citizens issued EDLs, thus, need not be restricted to any mode of travel, to include air. If the EDL were adopted nationwide to upgrade REAL ID compliant driver's licenses, in fact, all drivers' licenses would be authenticable and the restriction on commercial air travel would no longer be of any consequence. Since state and individual concerns have been addressed with an encrypted short-range or Smart Card ID, it is a long-term possibility. Without change, however, the long-term possibility is lost.

4. National ID Issues

Any change to a state ID system will invigorate the national ID debate, which REAL ID revealed. The DHS has indicated that the federal government has no intention of creating a *de facto* national ID as a consequence of REAL ID.[247] Database collection and information exchange, however, has made the need for national ID nearly moot as the underbelly of a formidable *de facto* NIDS already exists, especially when most activities, to include employment, are controlled by an ID system.[248] Such laws as the Privacy Act of 1974 or the Health Insurance Portability and Accountability Act of 1996

---

[246] John Pike, "Homeland Security: Biometrics," GlobalSecurity.org, http://www.globalsecurity.org/security/systems/biometrics.htm (accessed September 19, 2012).

[247] "Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes [73 FR 5271][FR 5-08]."

[248] Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 319.

do, however, protect *de facto* NIDS from abuse. More importantly, the taboos associated with a national ID are too strong for Congress to entertain the idea of requiring all U.S. citizens to be carded.

The underlying question is whether or not the adoption of an encrypted short-range RFID and/or Smart Card EDL is a national ID concern. As a voluntary ID, no identifiable concerns are evident. The national ID debate will be heightened, however, if adopted nationwide despite the fact that the EDL is and would remain a state function. Nonetheless, driver's licenses are a necessary ID system, are not mandatory, and already have and require machine-readable technology. Changing the type of technology, thus, has little to do with the national ID debate, which exists at the system level. The debate will fundamentally come down to the choices. Because RFID is RFID, the only viable secure and authenticable option is the Smart Card. Although more expensive to support two technical systems, having options does ring well with those who do not want to be imposed or outright fear RFID (RFID on/off switch may be a one technology solution).

5. Privacy Risks at the System Level

Converting to an encrypted short-range and/or Smart Card solution does not increase the privacy risks at the system level. By closing the security loop with an encrypted EDL, however, it does decrease the risks that can subvert the system to include privacy. Reducing and/or eliminating the number of IDs in support of the WHTI will also minimize system level risks. Importantly, adoption can only increase system-level protections and create other possibilities to further privacy protections.

B. ECONOMIC ASSESSMENT

Any change in technology to the EDL will have an economic consequence for citizens, either directly to the individual pocket book or indirectly in the form of taxes, or inflation. States and the federal government, thus, must consider these consequences when deciding on a technological change that could impact thousands of U.S. citizens. Above these consequences is another concern, specifically, a huge multi-trillion dollar

and growing deficit. States too have similar overarching problems.[249] Course corrections, thus, will not be joyful despite the convenience of a more secure driver's license that offers more privacy.

Although adopting the encrypted short-range RFID or Smart Card solution is seemingly costly up front, there is the back-end cost of continuing with a program that leads to a dead end when, for example, several states have already denied and/or placed restrictions on the current technical solution for the EDL.[250] In also does not make much sense to continue funding a program that can be subverted easily by counterfeits. More importantly, a course correction in the future will be more politically and economically costly.

The impact to commerce, trade, and tourism is another factor. The Canadian government, for example, has already complained of a "thickening" of the border as a consequence of the WHTI, reporting a roughly 30-percent drop in trade between the United States due to wait times at the border.[251] The EDL is not, as of late, the big player and as such, a change to technology to a voluntary program should be minimal. If the program is taken a step further to upgrade REAL ID compliant driver's licenses and to eliminate the WHTI, however, this factor is worth considering, particularly the time it takes to reach out a window.

C. REAL ID LIMITATIONS ASSESSMENT

The two major limitations identified for the current REAL ID complaint driver's license were the lack of a design standard for driver's licenses and an increased likelihood of counterfeiting as a result of state-wide improvements to the driver's license acquisition process as a result of REAL ID. With an encrypted short-range RFID or Smart Card solution, both of these issues are addressed. Both offer a quick, secure, more

---

[249] Jonathan Masters, "Why the Fiscal Health of States and Cities Matters," Council on Foreign Relations, http://www.cfr.org/economics/why-fiscal-health-states-cities-matters/p29198 (accessed October 21, 2012).

[250] "State Statutes Relating to Radio Frequency Identification (RFID) and Privacy"

[251] "Finding the Balance: Shared Border of the Future." The Canadian Chamber of Commerce, https://www.uschamber.com/sites/default/files/reports/0907_sharedborder.pdf (accessed September, 20, 2012).

private, and, thus, more practical means of authenticating IDs that are more difficult to counterfeit and minimally impact commerce. Both limitations, thus, are addressed while improving national security and individual privacy.

D. TECHNOLOGICAL ASSESSMENT

The EDL, as designed, has qualities that make it a unique ID beyond the unique RFID numbers it loosely emits. In fact, it is far more unique than any of the other WHTI border control documents—PASS card, SENTRI, FAST, NEXUS, Global Entry—as it supplants the staple ID U.S. citizens use to prove their identity in numerous settings. This versatility further increases the value of the EDL to terrorists beyond other WHTI IDs as well as the REAL ID compliant driver's license. The uniqueness calls for special attention to security.

Although REAL ID compliant driver's licenses alone are susceptible to counterfeiting, EDLs are more susceptible as a result of placing "Enhanced" on driver's license. The belief will be that intelligence, law enforcement, and other agencies will be less suspicious of someone with an EDL because of the implied security features. Without encryption and no authentication currently conducted beyond land and sea borders (a reason to *minimize* the number of border IDs types and *increase* authentication checks whenever and wherever possible), EDLs are more vulnerable.

EDLs are also more vulnerable as a result of their read range. In fact, long read-range on an ID has little, if anything, to do with security and will require countermeasures (driver's license plate recognition technology at borders, protective sleeve, additional authentication). Long-range RFID, thus, produces vulnerabilities if on a common and multiuse ID. Warriors down range who carry driver's licenses in their pocket, for example, could be "targeted" for an improvised explosive device (IED) attack. Similarly, political leaders, corporate titans, and other high-value targets could be vulnerable to targeting. As the 9/11 Commission pointed out, adversaries will exploit U.S. vulnerabilities and as such, there is no need to create them.

The following are the key reasons for an encrypted short-range and/or Smart Card solution:

- The EDL is a multiuse document often carried on person, used regularly, and not specific to border security. Like an e-passport, it is an extremely valuable ID to clone and counterfeit.
- The EDL's RFID serial numbers and TID serial numbers are more easily cloned by malicious readers without encryption, which increase the likelihood of counterfeiting.
- The EDL's long read range and multiuse nature, combined with pocket sleeve vulnerably, increases the likelihood of cloning and counterfeiting and other vulnerabilities.

To be effective by all measures, the encrypted short-range RFID and/or Smart Card solution must protect the unique serial numbers from such clandestine activities as cloning, skimming, tracking, and profiling. Further, the technology should be authenticable, otherwise, there is no need to go beyond what REAL ID has, or continues, to accomplish. Specifically, the EDL program should be suspended if a secure solution(s) is not adopted.

Some have suggested that the EDL, as currently equipped, could be given with an off and on switch, which alleviates some of the privacy concerns and/or threats from RFID technology away from the border.[252] Yet, the on/off solution only addresses some of the privacy issues and not the security issues; the solution is still not encrypted. Thus, it would not make economic sense to pursue this course of action. The on/off switch, however, could be a plausible solution for border specific IDs with long-range RFID, notably those that are not multipurpose and necessary for national security.

E. PRIVACY ASSESSMENT

Border control is a critical component of national security, yet so too are the ideals the border protects. Because obtaining the EDL is currently voluntary, the EDL must accord a level of privacy that is commensurate with the Fourth Amendment. In light

---

[252] Ann Cavoukian, "Adding an on/Off Device to Activate the RFID in Enhanced Driver's Licenses: Pioneering a made-in-Ontario Transformative Technology that Delivers both Privacy and Security," Information and Privacy Commissioner of Ontario, http://www.ipc.on.ca/images/Resources/edl.pdf (accessed September 20, 2012).

of a need for identification, the following are considered the key reasons for increase privacy protections:

- The EDL is more vulnerable to the threats associated with RFID due to its multiuse, which "increases an individual's likelihood of suffering dignitary harms as well as monetary or physical harms."[253]
- The EDL's RFID serial number and TID serial number more easily skimmed as a result of having long read-range and no encryption, which increase privacy threats to U.S. citizens.
- The EDL's privacy protection measures—protective sleeve, privacy awareness training—are inadequate to protect a multiuse driver's license.

The counter-argument for additional privacy protections also invokes the EDLs voluntary nature: Citizens can choose convenience over privacy. Critics may also argue that cell phones are just as or more susceptible, which they are.[254] A cell phone, however, can be turned off and battery removed to make it untrackable; of course, a cell phone is not required for "official purposes." Importantly, voluntary EDLs do not take into account the erosion of privacy implied in this relationship; erosion at the bottom of the mountain will lead to landslides that eventually destroy the mountain. The convenience and slightly cheaper cost, in fact, fuels the erosion process by incentivizing U.S. citizens to cash in their privacy.

253 Solove, *A Taxonomy of Privacy*, 485.

254 Leo Xavier, "Hackers can Easily Track Your Mobile Phone, Says Study (Video)," Mobile Magazine, http://www.mobilemag.com/2012/02/17/hackers-can-easily-track-your-mobile-phone-says-study-video/ (accessed October 21, 2012).

VI. RECOMMENDATIONS

Rooted in cost savings and convenience, the voluntary EDL, as currently equipped, cannot be justified under the rubric of national security. Other IDs—SENTRI card, FAST card, NEXUS card, PASS Card, Global Entry, and the U.S. passport—that are specific to border security could supplant the EDL with little, if any, long-term impact to commerce, trade, or tourism. In fact, there is little need for IDs beyond the e-passport and one WHTI card that identifies privileges. The recommendation, thus, is to begin reducing the number of WHTI IDs to increase authentication of a core ID, which decreases the likelihood of counterfeiting and increases the ability to detect visual anomalies. The core ID recommended: the EDL equipped with an encrypted short-range RFID or Smart Card technology.

Although the current unencrypted long-range EDL does more accurately reflect identity than REAL ID compliant driver's licenses, the technological solution does not account for the multiuse nature of a driver's license. Attached to a multiuse ID that is carried on person often and exposed regularly for proof of identity increases the threats of cloning, tracking, skimming, and profiling by malicious readers. As a voluntary ID, these threats are not justifiable under the umbrella of national security and increase other vulnerabilities. Further, incentives—money, power, influence, subverting security, etc.—are greater on a multiuse ID and as such, security measures must be commensurate. The recommendation, thus, is to adopt an encrypted short-range RFID or Smart Card solution to secure the EDL.

Similarly, the unencrypted long-range voluntary EDL does not adequately protect privacy and will increasingly contribute to a societal erosion of privacy. Attached to a multiuse ID that is carried on person often and exposed regularly for proof of identity it increases the threats of tracking, skimming serial numbers to understand individual predilections, identity theft, and profiling by malicious readers. As a voluntary ID, again, these threats are not justifiable under the umbrella of national security. Although much is contingent on ingenuity, such as generating reasons for individual's to pull their EDL out of the protective sleeve or increasing malicious reader power output to increase read

range, the threats are greater than the benefits the voluntary EDL offers. Further, the current technology is a barrier to full EDL acceptance.

Adopting an encrypted short-range RFID or a Smart Card solution or both for the purpose of upgrading REAL ID compliant driver's licenses that lack adequate Level 1 and 2 counterfeit protections provides the national security justification for the EDL program. Irrespective, the new solution(s) safeguards the right to privacy and as such, the program could also remain voluntary in support of the WHTI with a long-term outlook. Short economic expense; adoption is a win-win-win for the federal government, states, and U.S. citizens with the following benefits:

- New solution(s) reduces the ability to counterfeit a driver's license.
- New solution(s) decreases the likelihood of identity theft.
- New solution(s) reduces threats to Fourth Amendment privacy, especially if other long-range RFID IDs in support of WHTI are reduced or eliminated as a result.
- New solution(s) reduces system level threats to further security and privacy.
- New solution(s) allows biometrics to be stored on ID, if necessary, in the future.
- New solution(s) in-line with the Tenth Amendment or more fundamentally, the principles of federalism; EDL also remains state designed.
- New solution(s) utilizes "pull" option, which eliminates the need to mirror PII in two government databases.
- New solution(s) increases capabilities to states, particularly the ability to more securely store PII on a driver's license.
- New solution(s) reduces collation of PII in a federal database in support of the WHTI and thus, reduces national ID fears.
- New solution(s) is friendlier to the First Amendment as it reduces the need to mandate one biometric and reduces the "chilling effect" of long-range RFID.
- New solution(s) allows unfettered land, sea, and approved air border crossings with a driver's license that can still remain "optional" for that purpose.
- New solution(s) offers interoperability, speed, and precision, thus, are more practical in the field for ensuring security and commerce.

- New solution(s) increases public safety.

The question is where to begin. The first recommendation is to suspend the EDL program until a new solution(s) is adopted. Suspending the program will ensure funds are not spent unnecessarily. EDLs that are in service should be recalled. Risk analysis, however, may produce an alternative course of action; that is, the current EDLs may fade away, alleviating pressure on individual pocketbooks. If risk is accepted, EDLs that remain in circulation must be closely examined; aging of the EDL will increase the demand. Once a technical solution(s) is decided upon, the voluntary program should be reinitiated while seeking nationwide acceptance to seize the long-term benefits of a REAL EDL. New EDLs must be distinguishable from old EDLs if allowed to remain in circulation.

Congress must also enact federal legislation on the permissible uses of RFID for human IDs. The threats of RFID technology should not be pushed to the states, particularly when RFID technology is employed to support human ID initiatives by the federal government.

This thesis has advanced an argument that the EDL, after adopting the appropriate technology, represents less of an impact on the First Amendment, the Fourth Amendment, and the Tenth Amendment. Furthermore, it decreases the ability to counterfeit driver's license that is commensurate with acquisition hardening, decreases the potential for identity theft, increases interoperability to facilitate both security and commerce, holistically increases national security, decreases threats to individual privacy, reduces system level threats, and returns freedoms to U.S. citizens such as having the option to cross borders with a driver's license.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

"18 USC 2721 - Prohibition on Release and use of Certain Personal Information from State Motor Vehicle Records." Cornell University Law School. http://www.law.cornell.edu/uscode/text/18/2721 (accessed September 20, 2012).

"37.19 Machine Readable Technology on Driver's License Or Identification Card." U.S. Citizenship and Immigration Services. http://www.uscis.gov/ilink/docView/6CFR/HTML/6CFR/0–0–0–1/0–0–0–4972/0–0–0–5292.html (accessed September 20, 2012).

"About the Tenth Amendment." Tenth Amendment Center. http://tenthamendmentcenter.com/about/about-the-tenth-amendment/ (accessed September 20, 2012).

"ACLU Says Enhanced Driver's Licenses are Insecure, Fail to Protect Personal Information." American Civil Liberties Union. http://www.aclu.org/technology-and-liberty/aclu-says-enhanced-driver's-licenses-are-insecure-fail-protect-personal-infor (accessed May 26, 2012).

"The Basics of RFID Technology." RFID Journal. http://www.rfidjournal.com/article/articleview/1337/1/129/ (accessed September 20, 2012).

"Biometrics: Who's Watching You?" Electronic Frontier Foundation. https://www.eff.org/wp/biometrics-whos-watching-you (accessed September 20, 2012).

"Call to Action: The Growing Epidemic of Counterfeit Identity Documents and Practical Steps to Combat It." Document Security Alliance. http://www.documentsecurityalliance.com/forms/counterfeit_solutions.pdf (accessed October 21, 2012).

"Card Format Passport; Changes to Passport Fee Schedule." *Federal Register* 72, no. 249 (December 31, 2007): 74170.

"CBP's Trusted Traveler Systems using RFID Technology Require Enhanced Security (Redacted)." Department of Homeland Security Office of Inspector General. http://www.oig.dhs.gov/assets/Mgmt/OIGr-06–36_May06.pdf (accessed September 20, 2012).

"Comparing Security of E-Passport and Passport Card/Enhanced Driver's License." Center For Democracy & Technology. https://www.cdt.org/security/identity/20071231passcard.pdf (accessed September 20, 2012).

"Creating a Trusted Information Network for Homeland Security: Second Report of the Markle Foundation Task Force." *Markle Foundation*, 2003. http://www.markle.org/sites/default/files/nstf_report2_full_report.pdf (accessed September 20, 2012).

"Documents Required for Travelers Departing from Or Arriving in the United States at Air Ports-of-Entry from within the Western Hemisphere." *Federal Register* 71, (November 24, 2006): 68412. https://www.federalregister.gov/articles/2006/11/24/06–9402/documents-required-for-travelers-departing-from-or-arriving-in-the-united-states-at-air (accessed September 19, 2012).

"Driver Licensing Fees." Washington State Department of Licensing. http://www.dol.wa.gov/driverslicense/fees.html (accessed September 19, 2012).

"Driver's License & State ID: Enhanced Driver's License Fee Chart." Michigan Department of State. http://www.michigan.gov/sos/0,1607,7–127–1627_8669_9040–213056--,00.html (accessed September 19, 2012).

"Enhanced Driver's Licenses: What are they?" Homeland Security. http://www.dhs.gov/enhanced-drivers-licenses-what-are-they (accessed September 19, 2012).

"ePassport." Digital Locksmiths. http://www.digitallocksmiths.com/ePassport.html (accessed September 19, 2012).

"Expanding Civil Rights." PBS. http://www.pbs.org/wnet/supremecourt/rights/landmark_roe.html (accessed August 27, 2012).

"FAQs about Enhanced Driver's Licenses and Enhanced Non-Driver Photo ID Cards." New York Department of Motor Vehicles. http://www.dmv.ny.gov/edl-faqs.htm (accessed September 19, 2012).

"FAST Fact Sheet." Customs Border Patrol. http://www.cbp.gov/xp/cgov/travel/trusted_traveler/fast/fast_fact_sheet.xml (accessed September 19, 2012).

"Finding the Balance: Shared Border of the Future." The Canadian Chamber of Commerce. https://www.uschamber.com/sites/default/files/reports/0907_sharedborder.pdf (accessed September 20, 2012).

"FIPS PUB 46–3; Data Encryption Standards." U.S. Department of Commerce, National Institute of Standards and Technology. http://csrc.nist.gov/publications/fips/fips46–3/fips46–3.pdf (accessed September 20, 2012).

"FRAM Embedded 13.56 Mhz RFID LSI." FIND. http://www.fujitsu.com/downloads/EDG/binary/pdf/find/30–3e/5.pdf (accessed September 20, 2012).

"Get Your EDL/EID." Washington State Department of Licensing. http://www.dol.wa.gov/driverslicense/edlget.html (accessed May 12, 2012).

"How Companies are 'Defining Your Worth' Online." NPR. http://www.npr.org/2012/02/22/147189154/how-companies-are-defining-your-worth-online (accessed August 27, 2012).

"How does a Magnetic Stripe on the Back of a Credit Card Work?" howstuffworks. http://money.howstuffworks.com/personal-finance/debt-management/magnetic-stripe-credit-card1.htm (accessed September 20, 2012).

"Implementing 9/11 Commission Recommendations." U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/implementing-9–11-commission-report-progress-2011.pdf (accessed September 19, 2012).

"Inspection of the Secure Electronic Network for Travelers' Rapid Inspection." USDOJ/OIG. http://www.justice.gov/oig/reports/INS/e0019/bckgnd.htm (accessed September 19, 2012).

"License/Permit/ID Fees: Payment Information." Vermont Department of Motor Vehicles. http://dmv.vermont.gov/fees/license-permit-id (accessed September 19, 2012).

"Machine Readable Travel Documents, Part 1, Volume 2." International Civil Aviation Organization. http://hasbrouck.org/documents/ICAO9303-pt1-vol2.pdf (accessed September 19, 2012).

"Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes [73 FR 5271][FR 5–08]." Office of the Secretary, DHS. http://www.uscis.gov/ilink/docView/FR/HTML/FR/0–0–0–1/0–0–0–145991/0–0–0–165820/0–0–0–176819.html.

"Mission & Vision." NLETS. https://www.nlets.org/mission-vision (accessed October, 21, 2012).

"NASCIO Recognition Award Nomination." NASCIO. http://www.nascio.org/awards/nominations/2009/2009WA2-NASCIO%20AWARD%20INFORMATION%202009%20for%20EDL%20ID%20project_Final.pdf (accessed September 19, 2012).

"NEXUS Eligibility and Fees." Customs Border Patrol. http://www.cbp.gov/xp/cgov/travel/trusted_traveler/nexus_prog/nexus_eligibility.xml (accessed September 19, 2012).

"Overview of Enhanced Driver's License." Homeland Security. http://www.cbp.gov/linkhandler/cgov/travel/vacation/enhanced_dl_fs.ctt/enhanced_dl_fs.pdf (accessed May 9, 2012).

"Participation: Risk Based Security Initiative." Transportation Security Administration. http://www.tsa.gov/what_we_do/participation.shtm (accessed September 19, 2012).

"Passport Fees." U.S. Department of State. http://travel.state.gov/passport/fees/fees_837.html (accessed September 19, 2012).

"Personal Identification - AAMVA North American Standard - DL/ID Card Design." AAMVA. http://www.granddriver.info/uploadedFiles/MainSite/Content/SolutionsBestPractices/BestPracticesModelLegislation(1)/DLIDCardDesignStandard2011.pdf (accessed October 21, 2012).

"Proximity Range - ISO/IEC 14443." Infineon. http://www.infineon.com/cms/en/product/chip-card-and-security-ics/contactless-memory-and-rfid-products/proximity-range-iso/iec-14443/channel.html?channel=db3a3043294a35580129643635c95140 (accessed September 20, 2012).

"Radio Frequency Identification (RFID) Systems." Electronic Privacy Information Center. http://epic.org/privacy/rfid/ (accessed September 18, 2012).

"REAL ID State Legislation Database." National Conference of State Legislatures. http://www.ncsl.org/issues-research/transport/real-id-state-legislation.aspx (accessed September 18, 2012).

"RFID and RF Memory Products Based on ISO 14443 and ISO 15693." STMicroelectronics. http://www.st.com/Internet/com/SALES_AND_MARKETING_RESOURCES/MARKETING_COMMUNICATION/FLYER/flrfidrf.pdf (accessed September, 20, 2012).

"The Right of Privacy." University of Missouri Kansas City. http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html (accessed August 27, 2012).

"Samsung Announces High Performance Smart Card IC with 90-Nonometer Technology." Samsung. http://www.samsung.com/global/business/semiconductor/news-events/press-releases/detail?cateSearchParam=N011&searchTextParam=&startYyyyParam=&startMmParam=&endYyyyParam=&endMmParam=&newsId=4046&page=&searchType=C&rdoPeriod=A (accessed September 20, 2012).

"Secure Identification: The REAL ID Act's Minimum Standards for Driver's Licenses and Identification Cards." http://judiciary.house.gov/hearings/printers/112th/112–103_73416.PDF (accessed September 18, 2012).

"SENTRI Program Description." Customs Border Patrol. http://www.cbp.gov/xp/cgov/travel/trusted_traveler/sentri/sentri.xml (accessed September 19, 2012).

"Smart Border Alliance: RFID Feasibility Study Final Report." U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/foia/U.S.-VISIT_RFIDattachD.pdf (accessed September 20, 2012).

"State Statutes Relating to Radio Frequency Identification (RFID) and Privacy." National Conference of State Legislatures. http://www.ncsl.org/issues-research/telecom/radio-frequency-identification-rfid-privacy-laws.aspx (accessed August 22, 2012).

"Texas Instruments Expands Tag-it ISO/IEC 15693 RFID Product Line." PR Newswire. http://www.prnewswire.com/news-releases/texas-instruments-expands-tag-it-isoiec-15693-rfid-product-line-67541897.html (accessed September 20, 2012).

"Title 6 - Homeland Security 6 CFR Part 37: 37.15 Physical Security Features for the Driver's License Or Identification Card." Department of Homeland Security. http://uscis.gov/ilink/docView/6CFR/HTML/6CFR/0–0–0–1/0–0–0–4972/0–0–0–5202.html (accessed September 20, 2012).

"Title XX Transportation: Chapter 236 Highway Regulation, Protection and Control Regulations: Highway Video Surveillance." New Hampshire General Court. http://www.gencourt.state.nh.us/rsa/html/XX/236/236–130.htm (accessed September 20, 2012).

"TRF7960 Evaluation Module: ISO 15693 Host Commands." Texas Instruments. http://www.ti.com.cn/cn/lit/an/sloa141/sloa141.pdf (accessed September 20, 2012).

"Trusted Traveler Programs." Customs Border Patrol. http://www.cbp.gov/xp/cgov/travel/trusted_traveler/ (accessed September 19, 2012).

"Trusted Traveler Programs." Homeland Security. http://www.dhs.gov/trusted-traveler-programs (accessed October 21, 2012).

"The U.S. Electronic Passport." U.S. Department of State. http://travel.state.gov/passport/passport_2498.html (accessed September 19, 2012).

"The U.S. Electronic Passport Frequently Asked Questions." U.S. Department of State. http://travel.state.gov/passport/passport_2788.html (accessed September 19, 2012).

"U.S. Passport Card." U.S. Department of State. http://travel.state.gov/passport/ppt_card/ppt_card_3926.html (accessed September 19, 2012).

"U.S. seen as Less Important, China as More Powerful: Isolationist Sentiment Surges to Four-Decade High." Pew Research Center. http://www.people-press.org/2009/12/03/section-7-threat-of-terrorism-and-civil-liberties/ (accessed May 26, 2012).

"The use of RFID for Human Identification: A DRAFT REPORT from DHS Emerging Applications and Technology Subcommittee." Homeland Security. http://seattletimes.nwsource.com/news/business/links/rfidprivacy.pdf (accessed May 9, 2012).

"Washington, Hew Hampshire, and South Carolina Oppose Real ID." North Country Gazette. http://www.northcountrygazette.org/articles/2007/040807SixOppose.html (accessed September, 19, 2012).

"Western Hemisphere Travel Initiative." Customs Border Patrol. http://www.getyouhome.gov/html/rfid/RFID.html (accessed September 19, 2012).

"Western Hemisphere Travel Initiative." Homeland Security. http://www.dhs.gov/western-hemisphere-travel-initiative (accessed October 21, 2012).

"Western Hemisphere Travel Initiative: Designation of Enhanced Driver's Licenses and Identity Documents Issued by the States of Vermont and Michigan and the Provinces of Quebec, Manitoba, British Columbia, and Ontario as Acceptable Documents to Denote Identity and Citizenship." The Federal Register. www.federalregister.gov/articles/2009/05/29/E9–12513/western-hemisphere-travel-initiative-designation-of-enhanced-drivers-licenses-and-identity-documents (accessed May 11, 2012).

"Western Hemisphere Travel Initiative: Land and Sea Travel Document Requirements." U.S. Customs and Border Protection. http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/travel/whti_state_factsheet.ctt/whti_state_factsheet.pdf (accessed May 11, 2012).

"Whitepaper: EPCglobal Class 1 Gen 2 RFID Specification." ALIEN. http://www.alientechnology.com/docs/AT_wp_EPCGlobal_WEB.pdf (accessed September 20, 2012).

"WHTI: Special Groups." Customs Border Patrol. http://www.getyouhome.gov/html/lang_eng/eng_sa.html (accessed September 19, 2012).

"Why the Enhanced Driver's License is Wrong for California." American Civil Liberties Union of Northern California. https://www.aclunc.org/issues/technology/asset_upload_file944_8427.pdf (accessed August 27, 2012).

Abawajay, Jemal. "Enhancing RFID Tag Resistance Against Cloning Attack." *IEEE Computer Society* (2009): 18.

Aigner, Manfred, Burbridge, Trevor, Ilic, Alexander, Lyon, David, Soppera, Andrea and Lehtonen, Mikko. "White Paper: RFID Tag Security." Bridge. http://www.bridge-project.eu/data/File/BridgesecuritypaperDL_9.pdf (accessed September 20, 2012).

Albrecht, Katherine. "RFID TAG - YOU'RE IT." *Scientific American* 299, no. 3 (September, 2008): 72.

———. *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID*. Nashville, Tennessee: Nelson Communications, Inc, 2005.

Homeland Security Act of 2002, Public Law 107–296, (2002): 101.

Baliles, Gerald, Douglas Kmiec, K. Taipale, John Alderdice, and Marc Rotenberg. *Public Debate Resolution: In the War Against Terrorism, and with Advances in Technology, Americans Need to Lower their Expectations of Privacy*. University of Virginia: Miller Center of Public Affairs, 2007.

Bean, Hamilton. “Exploring the Relationship between Homeland Security Information Sharing & Local Emergency Preparedness.” *Homeland Security Affairs* 5, no. 2 (May, 2009).

Bell, Tom. “Restatement (Second) of Torts: 652A-E (1997).” Tomwbell.com. http://www.tomwbell.com/NetLaw/Ch05/R2ndTorts.html (accessed August 27, 2012).

Bertoni, Daniel. *Driver’s License Security: Federal Leadership Needed to Address Remaining Vulnerabilities*: United States Government Accountability Office, 2012.

Brown, Mary. “Security Challenges in RFID Implementations.” *The ISSA Journal* (May, 2006): September 19, 2012.

Bush, Steve. “HP Passive RFID Chip Targets High Capacity Storage.” Electronics Weekly. http://www.electronicsweekly.com/Articles/24/07/2006/39301/HP-passive-RFID-chip-targets-high-capacity-storage.htm (accessed August 27, 2012).

Caldwell, Dave. “A Look at Your License.” Minot Daily News. http://www.minotdailynews.com/page/content.detail/id/550887.html (accessed September 20, 2012).

Cate, Fred. “Government Data Mining: The Need for a Legal Framework.” *Harvard Civil Rights-Civil Liberties Law Review* 43, (2008): 435.

Cavoukian, Ann. “Adding an on/Off Device to Activate the RFID in Enhanced Driver’s Licenses: Pioneering a made-in-Ontario Transformative Technology that Delivers both Privacy and Security.” Information and Privacy Commissioner of Ontario. http://www.ipc.on.ca/images/Resources/edl.pdf (accessed September 20, 2012).

Cialdini, Robert B. *Influence: The Psychology of Persuasion*. EPub ed. HarperCollins, 2009.

Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108–796, (2004): 1001.

Davenport, Thomas, Mule, Leandro D. and Lucker, John. “Know what Your Customers Want Before they Do.” Harvard Business Review. http://theinformationdj.com/wp-content/uploads/2012/02/know-what-your-customer-wants-before.pdf (accessed August 27, 2012).

Davis, Darren and Brian Silver. “Civil Liberties Vs. Security: Public Opinion in the Context of the Terrorist Attacks on America.” *American Journal of Political Science* 48, no. 1 (January, 2004): 28.

Finkenzeller, Klaus. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. Translated by Rachel Waddington. Second ed. New Jersey: Wiley, 2006.

Finklea, Kristin. "Identity Theft: Trends and Issues." Congressional Research Service. http://www.fas.org/sgp/crs/misc/R40599.pdf (accessed September, 20, 2012).

Glancy, Dorothy J. "The Invention of the Right to Privacy." *Arizona Law Review* 21, no. 1 (1979a)

Gosset, Nathalie. "What is ISO 14443?" eHow. http://www.ehow.com/about_6591701_iso-14443_.html (accessed September 20, 2012).

Greene, Tim. "Bad Guys could Read RFID Passports at 217 Feet, Maybe a Lot More." Network World. http://www.networkworld.com/news/2010/072910-black-hat-rfid-passports.html (accessed September 20, 2012).

Haber, Gary. "Angelos, Murphy Sue Facebook Over Privacy Rights." Baltimore Business Journal. http://www.bizjournals.com/baltimore/news/2012/02/22/baltimore-law-firms-sue-facebook-over.html (accessed August 22, 2010).

Hancke, Gerhard. "A Practical Relay Attack on ISO 14443 Proximity Cards." Gerhard Hancke, University of Cambridge, Computer Laboratory. http://www.rfidblog.org.uk/hancke-rfidrelay.pdf (accessed September, 20, 2012).

Himberger, D., D. Gaylin, T. Tompson, J. Agiesta, and J. Kelly. "Civil Liberties and Security 10 Years After 9/11." *The Associated Press-NORC Center for Public Affairs Research*, September 2011.

Dwyer v. American Express Company, 652 N.E. 2d, 1351 (Appellate Court of Illinois, First District, First Division 1995).

Holloway, Simon. "Real Time Location Systems are the New Buzz in RFID." The Register. http://www.theregister.co.uk/2007/08/21/aeroscout_location_systems/ (accessed September 18, 2012).

Hornyak, Tim. "RFID Powder." *Scientific American* (February, 2008): 68.

Hoven, Michael. "United States V. Skinner: Sixth Circuit Approves Warrantless Tracking of Cell Phone Location." JOLT Digest. http://jolt.law.harvard.edu/digest/telecommunications/united-states-v-skinner (accessed October 6, 2012).

Hudson, Audrey. "Napolitano Debates REAL ID." *The Washington Times*, February 20, 2009.

Identity Theft and Assumption Deterrence Act of 1998, Public Law 4151, (1998): 105.

Ilie-Zudor, Elisabeth, Zsolt Kemeny, Peter Ergi, and Laszlo Monostori. *The RFID Technology and its Current Applications*. Department of Production Informatics, Management and Control, BME Hungary: The Modern Information Technology in the Innovation Processes of the Industrial Enterprises, 2006.

Jallad, Tarik. "Old Answers to New Questions: GPS Surveillance and the Unwarranted Need for Warrants." *North Carolina Journal of Law & Technology* 11, no. 2 (Spring, 2010): 351.

Jones, Neil. "RFID and the Difference between Passive and Active RFID Tags." Ezine Articles. http://ezinearticles.com/?RFID-and-the-Difference-Between-Passive-and-Active-RFID-Tags&id=3428256 (accessed August 27, 2012).

Juels, Ari, Molnar, David and Wagner, David. "Security and Privacy Issues in E-Passports." The California State Library. http://www.library.ca.gov/crb/rfidap/docs/JuelsetalI-SecurityandPrivacyofE-Passports.pdf (accessed August 27, 2012).

Kean, Thomas, Ben-Veniste, Richard, Fielding, Fred, Gorelick, Jamie, Gorton, Slade, Hamilton, Lee, Kerrey, Bob, Lehman, John, Roemer, Timothy and Thompson, James. "The 9/11 Commission Report." National Commission on Terrorist Attacks Upon the United States. http://www.9–11commission.gov/report/911Report.pdf (accessed September 18, 2012).

Kenner, Marty, Wilson, Bruce and Rhyner, Steve. "U.S. Driver's Licenses: Addressing the Potential Vulnerabilities." 3M. http://solutions.3m.com/3MContentRetrievalAPI/BlobServlet?lmd=1329168842000&locale=en_WW&assetType=MMM_Image&assetId=1319220855046&blobAttribute=ImageFile (accessed September 20, 2012).

Kephart, Janice L. "Identity and Security: Moving Beyond the 9/11 Staff Report on Identity Document Security." 911securitysolutions.com. http://www.911securitysolutions.com/index.php?option=com_contents&task=view&id=117&Itemid=38 (accessed April 27, 2012).

———. "REAL ID Implementation Annual Report: Major Progress made in Securing Driver's License Issuance Against Identity Theft and Fraud." *Backgrounder* (February, 2012): 11.

Kiefer, Heather. “Do Americans Want National ID Cards?” Gallop. http://www.gallop.com/poll/6364/americans-want-national-cards.aspx (accessed September 20, 2012).

Koscher, Karl, Brajkovic, Vjekoslav, Juels, Ari and Kohno, Tadayoshi. “EPC RFID Tag Security Weaknesses and Defenses: Passport Cards, Enhanced Drivers Licenses, and Beyond.” University of Washington. www.cs.washington.edu/homes/yoshi/papers/RFID/css280-koscher.pdf (accessed May 10, 2012).

Landt, Jeremy. “The History of RFID.” *IEEE Potentials* (October-November, 2005): 8–11.

Lehtonen, Mikko, Ostojic, Daniel, Ilic, Alexander and Michahelles, Florian. “Securing RFID Systems by Detecting Tag Cloning.” ETH. https://edit.ethz.ch/im/people/mlehtonen/ETH_SS_Pervasive09.pdf (accessed September 20, 2012).

Levy, Joshua. “Towards a Brighter Fourth Amendment: Privacy and Technological Change.” *Virginia Journal of Law & Technology* 16, no. 4 (Winter, 2011)

Lipowicz, Alice. “New Federal ID Cards Easily Cloned, Study Says.” Federal Computer. http://fcw.com/articles/2008/10/24/new-federal-id-cards-easily-cloned-study-says.aspx (accessed September 20, 2012).

Manaher, Colleen. “Privacy Impact Assessment for the use of Radio Frequency Identification (RFID) Technology for Border Crossings.” U.S. Department of Homeland Security. http://foia.cbp.gov/streamingWord.asp?i=45 (accessed September 20, 2012).

Markovich, Matt. “‘Near-Perfect” Fake IDs Pose Law Enforcement Challenge.” Komonews. http://www.komonews.com/news/local/Near-perfect-fake-IDs-pose-law-enforcement-challenge-153736705.html (accessed October 21, 2012).

Masters, Jonathan. “Why the Fiscal Health of States and Cities Matters.” Council on Foreign Relations. http://www.cfr.org/economics/why-fiscal-health-states-cities-matters/p29198 (accessed October 21, 2012).

McCallister, Erika, Tim Grance, and Karen Scarfone. “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).” *NIST, U.S. Department of Commerce* 800–122, (April, 2012): 2–1.

Mercer, John. “Breeder Documents.” *Keesing Journal of Documents & Identity* no. 29 (2009): 14–17.

Merserve, Jean and Ahlers, Mike. “9/11 Commission Members Act to Finally Wrap it Up.” CNN. http://cnn.com/2009/U.S./07/25/new.antiterror.group/index.html (accessed May 6, 2012).

Metheny, Matt. *Radio Frequency Identification Technology (RFID): Securing the Homeland through Next Generation Identification Technology*. Washington D.C.: Lunarline, Inc., 2006.

Migdal, Joel. *Strong Societies and Weak States*. New Jersey: Princeton University Press, 1988.

O’Connor, Mary. “EPC Tags Subject to Phone Attacks.” RFID Journal. http://www.rfidjournal.com/article/view/2167 (accessed October 21, 2012).

Ozer, Nicole A. “Rights “Chipped” Away: RFID and Identification Documents.” *Stanford Technology Law Review* 1, no. 1 (2008).

Pagnattaro, Marisa. “Getting Under Your Skin-Literally: RFID in the Employment Context.” *Journal of Law, Technology & Policy* 2, (2008): 237.

Pike, John. “Homeland Security: Biometrics.” GlobalSecurity.org. http://www.globalsecurity.org/security/systems/biometrics.htm (accessed September 19, 2012).

Prosser, William J. “Privacy.” *California Law Review* 48, no. 3 (1960): 390.

REAL ID Act of 2005, Public Law 109–13, (2005): H.R. 418.

Ricker, Thomas. “Video: Hacker War Drives San Francisco Cloning RFID Passports.” Engadget. http://www.engadget.com/2009/02/02/video-hacker-war-drives-san-francisco-cloning-rfid-passports/ (accessed September 20, 2012).

Rieback, Melanie, Crispo, Bruno and Andrew Tanenbaum. “The Evolution of RFID Security.” *Pervasive Computing* (January-March, 2006): 62–64.

Roberti, Mark. “The History of RFID Technology.” RFID Journal. http://www.rfidjournal.com/article/print/1338 (accessed September 19, 2012).

Saxhaug, Tom. “News Release: Enhanced Driver’s License Bill Passes Legislature.” Minnesota Senate. http://www.senate.mn/members/member_pr_display.php?ls=&id=3396 (accessed September 19, 2012).

Shilov, Anton. “T-Mobile to Exclusively Sell Apple iPhone in Germany for T399.” Xbit. http://www.xbitlabs.com/news/mobile/display/20070919164000.html (accessed October 21, 2012).

Smith, Alison M. “National Identification Cards: Legal Issues.” Congressional Research Service. http://assets.opencrs.com/rpts/RS21137_20030107.pdf (accessed October 21, 2012).

Smith, Jennifer. “You Can Run, but You Can’t Hide: Protecting Privacy from Radio Frequency Identification Technology.” *North Carolina Journal of Law & Technology* 8, no. 2 (Spring, 2007): 249.

Sobel, Richard. “The Demeaning of Identity and Personhood in National Identification Systems.” *Harvard Journal of Law & Technology* 15, no. 2 (Spring, 2002): 319.

Solove, Daniel J. “A Taxonomy of Privacy.” *University of Pennsylvania Law Review* 154, no. 3 (January, 2006)

Stanley, Jay and Steinhardt, Barry. “Even Bigger, Even Weaker: The Emerging Surveillance Society: Where are we Now?” American Civil Liberties Union. https://www.aclu.org/files/pdfs/privacy/bigger_weaker.pdf (accessed August 27, 2012).

Stein, Serena G. “Where Will Consumers Find Privacy Protection from RFIDS? A Case for Federal Legislation.” *Duke Law & Technology Review* 3, (2007).

Swedberg, Claire. “A Flurry of High-Memory Tags Take Flight.” RFID Journal. http://www.rfidjournal.com/article/view/8295 (accessed September, 20, 2012).

———. “MTI Creates EPC Gen 2 USB Reader for Retailer Applications.” RFID Journal. http://www.rfidjournal.com/article/view/7540/ (accessed August 27, 2012).

Tatelman, Todd B. *The REAL ID Act of 2005: Legal, Regulatory, and Implementation Issues*. Washington D.C.: Congressional Research Service, 2008.

Want, Roy. “An Introduction to RFID Technology.” *Pervasive Computing* (January-March, 2006): 25.

Warren, Samuel D. and Louis D. Brandeis. “The Right to Privacy.” *Harvard Law Review* 4, no. 5 (December 15, 1890): 193.

Williams, David. “REAL ID Still a REAL Mess.” Taxpayers Protection Alliance. http://www.protectingtaxpayers.org/index.php?blog&action=view&post_id=146 (accessed October 21, 2012).

Won, Kim and He-Joon Kim. “Smart Cards: Status, Issues, and U.S. Adoption.” *Journal of Object Technology* 3, no. 5 (May-June, 2004): 25–30.

Xavier, Leo. “Hackers can Easily Track Your Mobile Phone, Says Study (Video).” Mobile Magazine. http://www.mobilemag.com/2012/02/17/hackers-can-easily-track-your-mobile-phone-says-study-video/ (accessed October 21, 2012).

Yoshida, Junko. “Tests Reveal E-Passport Security Flaw.” Electronic Engineering Times. http://www.eetimes.com/electronics-news/4049950/Tests-reveal-e-passport-security-flaw (accessed September 20, 2012).

Zimmerman, Michael. “Biometrics and User Authentication.” SANS Institute. http://www.sans.org/reading_room/whitepapers/authentication/biometrics-user-authentication_122 (accessed October 21, 2012).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California